Cyber Terrorism and the SAFETY Act

By: Bob Karl, Managing Partner – SAFETY ACT CONSULTANTS

The Cyber Threatscape

The Internet has become a key element of day-to-day life. It is a critical tool for industry, finance, business, critical infrastructure, governments, military, research, science, and many other areas. Because of this new paradigm, cyber terrorism, e-crime, identity theft, espionage, sabotage are potentially some of the most dangerous types of risks faced today.

Regardless of time, dollars invested, and how well security initiatives are customized and deployed, all networks will eventually be compromised. Minimizing exposures to loss, damage, and the resulting financial liability is paramount to any organization. Proactive actions will help to maintain the organization's good reputation, normal business operations, protect the bottom line, and quite possibly, its financial survival.

The Terrorism Threatscape

Today's terrorists and extremist groups are highly motivated, keenly focused, opportunistic, and extremely adaptive. They are well funded, technologically advanced, and many have global networks capable of inflicting devastating damage to a wide range of targets including exploiting cyberspace. Many different types of entities remain targets. However, most focus on "industry norms" rather than the best solutions that address their unique needs and threats. Unfortunately, in cyberspace, these threats 'morph' daily and there will never be static solutions or norms.

Cyber Terrorism

A formal definition for "cyber terrorism" is still elusive and remains controversial. In general and in our opinion, cyber terrorism is the premeditated use of disruptive, covert, or malicious actions against computers, electronic networks, smart mobile or other external devices including memory devices, Its intent is to cause disruption, physical or financial harm to help further social, ideological, religious, political, or similar causes, objectives, and public opinion.

Cyber or e-terrorism can fall into many categories. The first, and very well exploited by Hollywood, would be hacking into a system in order to influence mechanical control and cause physical harm to people and/or property. Examples include open dams, shutting down power grids, causing highly dangerous situations in public transportation, at refineries, chemical or nuclear plants, etc.

The second type of cyber related terrorism is exploiting a network to cause immediate and direct financial harm targeted at a specific organization or sector. This could include out-and-out theft of funds, data, proprietary information, or to defraud others, espionage, compromise customer privacy and/or personal information, stock price manipulation, etc. The list of potentially damaging financial scenarios goes on and on.

Cyber Terrorism *Continued*

Other types of e-terrorism categories are more obscure, intertwined, and can easily be employed to help facilitate other types of attacks including the ones described above. These events, the ultimate damage, and any resulting liability may not be discovered for many years. These types of attacks include, but are certainly not limited to:

- **Raising Money** - Setting up electronic theft, fraud, money-laundering or other schemes to fund other terrorist activities such as recruiting, planning, and executing future attacks.
- **Using Malware** – Hacking into a network to plant Trojan Horses, spyware, viruses, or other malware assisting in theft, destruction, or manipulation of assets, funds, information or data.
- **Obtaining Remote Access** - Accessing a computer or network to gain "safe" web access. To avoid detection, terrorists communicate, plan, time events, purchase tickets, etc. under the guise of such activities originating from a trusted source. This could be your organization's network. Google: *"How to hack into a network,"* to see thousands of very scary results.
- **Identity Theft** - Terrorists use stolen identities to cover their actions and help elude detection. These identities also include "virtual identities" such network IP or email addresses. There are many benefits of stealing a virtual or online identity. Information gathering and planning can be made much easier by exploiting 'trusted' relationships when acting as the stolen identity. As an example, obtaining information from others as a 'trusted' email sender.
- **Manipulate Stock Prices** - Online stock trading and message boards have resulted in an environment where it is very possible to deliberately manipulate a stock's price. This is made even easier and ultra-transparent with the 'right' stolen identity. Terrorists can use this as an additional funding source, or to manipulate stock or commodity prices with the ultimate intent of moving markets into chaos. A virtual 'attack' on a given company's stock, rather than a physical attack on their facilities, could be highly effective. The planning and execution stages would be less detectable, and in particular, by using stolen identities through 'safe' networks.

Unlike "conventional" terrorism limited to physical attacks on hard targets, cyber threats:

- Have an almost infinite number of relatively easy access points
- Have a truly global reach from any location on earth
- Are more effective in relying on both true anonymity, and quite literally, light speed
- Transcend all physical, organizational, operational, geopolitical, and national borders
- Can target any stakeholder — individuals, schools, municipalities, corporations or other organizations, including entire industries, sectors, markets, economies, governments, etc.
- Can cause physical or financial harm, or both:
    - Can impact physical domains such as critical infrastructure or facility operations
    - Can be intended to cause, direct financial harm to specific targets

Terrorism and Liability Exposure

Any entity that uses, provides or is otherwise involved with security related products, technologies, procedures, or services, cyber or otherwise, and whether for themselves or others, does so at an extraordinary liability risk. Any serious terrorism / e-terrorism attack can result in a massive liability expense for any party deemed even partially responsible for not detecting, preventing, or mitigating the event. Victims will attempt to recover damages from any entity seen as potentially negligent. All security related equipment, technologies, protocols, decisions, procedures, services, assessments, and vulnerability studies, will be intensely scrutinized. Because of this potentially catastrophic risk, organizations have a responsibility to explore the broad immunities, liability caps, defenses, and other protections afforded under the SAFETY Act.

Terrorism Insurance as a Solution

Terrorism insurance remains available in the commercial marketplace. However, insurers view terror-related perils as catastrophic and unpredictable in nature. The premiums for "conventional" terrorism liability coverage can be prohibitive, and in particular, for e-terrorism liability coverage. If there is another terrorist attack in the US, it is very likely that any terrorism coverage you may have will become highly restrictive, economically unfeasible, or not available at all. This was the certainly case immediately following 9/11.

Today, regardless of premiums, the worldwide insurance marketplace does not have nearly enough total capacity necessary to provide adequate terrorism liability limits. In the event an organization is held even partially liable for damages from a serious terrorist event, it is highly likely they do not have enough insurance to effectively protect their bottom line. Insurance coverage alone is unlikely to assure financial survival after the emotionally charged and highly visible litigation that will certainly follow a terrorist attack. For a majority of organizations, SAFETY Act protection is by far the broadest, least expensive, and perhaps, the only solution.

The SAFETY Act

The SAFETY Act is a little known and often misunderstood Federal law that can protect an entity from the truly "enterprise threatening" liability they could face following a serious terrorist or-e-terrorist event. This Federal law was enacted by Congress as a part of the Homeland Security Act of 2002 (Public Law 107-296). The SAFETY Act is perhaps the most significant piece of Federal tort reform legislation ever enacted.

"SAFETY Act" is actually an acronym for the section of the Homeland Security Act titled the "Support Anti-terrorism by Fostering Effective Technologies Act". The Act's purpose is to ensure that the threat of potential liability suits does not limit or deter the use, development, deployment, or commercialization of products, technologies, procedures, hardware, software and/or services that could prevent or help mitigate a terrorist or e-terrorist attack.

SAFETY Act approval drastically reduces or eliminates the huge liability exposures an organization will face if a serious terrorism / e-terrorism attack somehow involves their facilities, products, technologies, procedures, systems, networks, hardware, or software.

SAFETY Act *Continued*

This Act provides unprecedented and sweeping immunities, liability protections, dollar caps, affirmative defenses, and other incentives for SAFETY Act approved entities that use or provide services, products or technologies that can help in identifying, preventing, deterring, mitigating, responding to, or recovering from, a terrorism or e-terrorism event.

The Act protects against allegations that a SAFETY Act Designated product, technology, service, procedure, etc. failed, was inadequate, ineffective, or otherwise did not help identify, prevent, respond to, respond appropriately, or otherwise help mitigate a terrorist act. Protections apply to suits alleging, bodily injury, property damage, or other harm, including liability for financial harm.

An eligible applicant does not have to be the manufacturer, developer, or seller of the products, technologies or services to benefit under this law. In fact, just by using another entity's SAFETY Act approved products, technologies, or services, the user is automatically immune from terrorism related suits alleging inadequacy, deficiency, or failure in such. No DHS application necessary!

In addition, to qualify for SAFETY Act protection, the products, technologies, services, or procedures do not have to be dedicated exclusively to defending against terrorism / e-terrorism. Access control, overall facility security procedures, and network protections are all eligible and ideal examples of simultaneously guarding against both terrorism and non-terrorism threats.

Although not the law's primary intent, entities that sell or provide security, anti-terrorism / e-terrorism goods, advice, or services to others enjoy a significant marketing advantage and higher demand for SAFETY Act approved products, technologies and services.

Summary & Key Take Aways

- Be realistic and proactive when analyzing your unique exposures – A reactive response in the case of terrorism or e-terrorism is way too late, and can threaten the entire enterprise.
- Understand your remote access, flash / portable memory, smart phone or other wireless device exposure - Remote access compromise is the primary attack vector employed.
- Use SAFETY Act Designated products or services, but only if they fulfill your specific needs and security requirements.
- Incorporate SAFETY Act requisites into your procurement / vendor / bidding process.
- Apply for your own SAFETY Act Designation(s) if, and as appropriate.
- Monitor SAFETY Act applicability and approvals for your vendors, providers, partners, etc.
- Designate a key person or team to be responsible for your organizational SAFETY Act strategies, goals, objectives, and internal expertise.
- If you do provide security or anti-terrorism solutions to others, use the SAFETY Act as one of the best competitive edges and marketing advantages you will ever have!

...

Get Into the Act™

SAFETY ACT CONSULTANTS

Phone: (202) 640-4000 - Toll Free (877) S ACT HELP

Fax: (202) 407-7054 - www.SAFETYACTCONSULTANTS.com