Cyber Terrorism and the SAFETY Act

By: Bob Karl, Managing Partner – SAFETY ACT CONSULTANTS for the Public Entity Risk Institute ("PERI")
Appeared in the Public Entity Risk Institute's "PERIScope" quarterly newsletter – Page 1 – January 14, 2011

Over the last two decades globalization has profoundly changed virtually all business models. Most of these changes are good; however, it has also increased both our vulnerability and exposure to new twenty first century threats. We have never been more dependent on critical infrastructure, and in particular, information systems.

We live and trade in a highly complex world. This complexity is creating new opportunities and, potentially catastrophic risks. Simply put, our risk management paradigm has not fully shifted to address the reality of the new world. Most risk management strategies are still based on simpler times when the risks were predictable, not nearly as complex, and the potential outcomes were clearer. Although those times were not very long ago, make no mistake, they are gone forever.

Today we are unconstrained in virtually every measure of information flow. Geography is no longer a barrier. Information moves freely across borders literally at light speed. Cost is not an issue. You can be poor and still have access to digital media and be able to make an impact on society, whether good or bad. Accessibility of sophisticated technology is no longer a constraint. Anyone with a cheap computer or even a cell phone can get online and communicate globally.

Cyber-attacks have now become one of the greatest threats from terrorists, radicals, and extremists. As the Internet becomes a larger and larger component of our lives, and a critical business tool, the problem worsens. The complexity, sophistication, and cost of fighting cyber-attacks is increasing constantly. Many say that attack sophistication, methods, and strategies way outpace the development and deployment of viable cyber defenses.

Facts

Executives at security firm McAfee Inc. say cyber threats are growing at an exponential rate. They report sampling some 34 million pieces of malware in 2010, more than double the 16 million in 2008. Currently, that translates into 47,000 pieces of such malicious code as Trojan Horses and viruses per day that are sent via email, delivered through USB drives, and through a telephone / smart phone connected to the Internet. *(McAfee Labs, 2010)*

The recent discovery of the Stuxnet worm has generated much concern from industry experts and IT security professionals. In November 2010 the U.S. government's senior cyber security expert from the DHS called the program a "game changer" in cyber warfare. The head of the DHS Cybersecurity Center, Sean McGurk, addressed the issue to the Senate Homeland Security Committee.

“We already knew Stuxnet was unprecedented, but it’s what is unknown about it that makes it so unsettling. The code can enter systems undetected, steal information or alter processes, and basically live there causing a mess of things while the system appears to security software to be working properly. But authorities don’t know where the Stuxnet worm came from, or what it was specifically designed to attack,” McGurk told Senators.

Attackers can use information made public about the Stuxnet worm to develop variations targeting other industries, affecting the production of everything from chemicals to baby formula. "This code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product, and indicate to the operator and your antivirus software that everything is functioning as expected."

The Stuxnet worm is a "wake-up call" because of its complexity and its aim at critical infrastructure systems, a Symantec director told a U.S. congressional committee in mid-November 2010. The malware is a milestone in many ways, Dean Turner, director of Symantec Security Response's Global Intelligence Network, said in testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs.

It is the first known threat to spy on, reprogram industrial control systems, and grant hackers control of critical infrastructures; use four zero-day vulnerabilities; compromise two digital certificates; inject code into industrial control systems and hide the code from operators; and include a programmable logic controller (PLC) rootkit to reprogram PLCs and hide the changes, he said. "Stuxnet is an incredibly large and complex threat," Turner said. "In fact, it is one of the most complex threats that we have ever analyzed to date at Symantec."

"Stuxnet demonstrates the vulnerability of critical national infrastructure industrial control systems to attack through widely used computer programs and technology. Stuxnet is a wake-up call to critical infrastructure systems around the world," he said. "Stuxnet has highlighted that direct attacks to control critical infrastructure are possible and not spy-novel fictions. The real-world implications of Stuxnet are beyond any threat we have seen in the past." *(Mills, 2010)*

The Threats Today

Twenty years ago, terrorism was unsophisticated, unorganized, localized, politically constrained and aimed at attempting to change national policies. Virtual or cyber terrorism did not exist. Today, threats are transnational, unconstrained and many are deeply rooted in cultural or religious beliefs. They can be highly organized cyber-attacks, physical attacks or both.

New terrorist organizations are highly funded, technologically savvy, determined and adapt quickly to new defenses. They are well-organized groups that are capable of inflicting devastating damage to a wide range of targets. You have to adapt your organizational strategies and behaviors to be in line with the complexity of the risks faced today, and in particular, within the cyber realm.

Hacking into IT systems is no longer limited to a bored teenage techie sitting in a basement somewhere in the US. Today, hacking is a tool used by unfriendly nations, radicals, extremists, terrorist groups as well as organized crime. Frequently, teams of people, each with a different skill set, join forces to attack systems from anywhere in the world.

Today's potential cyber risks and exposures are far more severe than just compromised personal information. Vulnerabilities in information systems threaten the entire country's physical and financial security and safety.

If you ask people what cyber terrorism is, you will get many different answers. If you ask the "experts", you will get twice as many answers. Despite the recent and intense media and government attention, there is no agreement as to what actions fall under "cyber terrorism". Keep in mind, computers and the Internet played key roles in the planning and execution of the September 11th attacks.

There are thousands of ways that terrorists can use the web as a very effective tool. I will try to group cyber terrorism into basic categories based on the ultimate intent of the attack. These are my "groupings" and my mission is not to "organize" threats into pre-defined boxes - it is to have you think about some of the methods employed to further the terrorists' causes. Just because your IT system is small, may not directly access or store certain information or control certain things, do not be lulled into complacency. It can still be used as a remote system to access the web or other networks as a "trusted" source.

The first of my categories of e-terrorism has been very well exploited by Hollywood. It is hacking into a system with the intent of causing, or threatening, physical harm to people or property. Examples include opening dams, shutting down power grids or causing highly dangerous situations in transportation systems, at refineries, chemical plants or other industrial facilities.

Another category is using IT systems with the direct intent of causing financial harm to an organization, industry, economy, government, etc.

Other e-terrorism categories are more obscure, intertwined, and can even be employed to help facilitate the types of attacks discussed above. These include:

- Setting up electronic theft, fraud, money-laundering, or similar schemes, to acquire money that is ultimately used to finance other terrorist activities such as propaganda, recruiting and new attacks.
- Remotely accessing a computer or network to gain 'safe' web access. The terrorists can then communicate, make travel plans and as an example, purchase airline tickets from a "safe" source to avoid detection. *Could this safe source be your organization's computers? Rare you may think? Try Googling: "how to hack remote access to network" and look at the thousands of results.*
- Hacking into a network to plant Trojan Horses, spyware, viruses, and malware for the theft, destruction or manipulation of data.

- Facilitating identity theft - Terrorists can, and most likely will, use stolen identities to cover their actions and help elude detection. These can also include virtual identities such as email addresses. *There are many benefits of stealing a user's online identity. Information gathering and attack planning can be made easier by exploiting 'trusted' relationships when logged in as the stolen identity or obtaining information 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 stock prices. This is made even easier and ultra-transparent with the 'right' stolen identity. Terrorist can use this as an additional funding source. This also includes attempts to manipulate stock or commodity prices with the ultimate intent of moving the market(s) into chaos. A virtual 'attack' on a given stock rather than a physical attack on a facility could be highly effective, and it's planning stage much less detectable, through stolen identities.

Any of these events creates massive liability exposures for any party that could be deemed even partially responsible for not detecting, preventing or at least mitigating the event. There is not enough insurance capacity globally to cover a serious terrorism or e-terrorism attack. The plaintiff's bar will be looking very hard at finding the many 'deep pockets' involved.

The Exposure Is Real

In October 2005, a six-member jury in New York State Supreme Court found that the Port Authority of NY NJ did not heed warnings that the World Trade Center underground garage was vulnerable to a terrorist attack and should be closed to public parking.

The jury found that the agency had not properly protected its underground public parking garage, where terrorists blew up a rental van loaded with explosives on Feb. 26, 1993. The Manhattan jury said that this failure was "a substantial factor" in allowing the bombing to occur. The bombing killed six people and injured 1,000. "Notably, the Port Authority has not cited any cases in which the court has held that a landlord may disregard its own knowledge about the likelihood of criminal activity and the warnings of its own security experts."

A motion to dismiss based on sovereign immunity was also denied by the court.

The 2005 jury apportioned more than half the blame to the Port Authority (68%). The terrorists were apportioned only 32% of the total liability. Under New York State law, once a defendant is more than 50 percent at fault, he/she/it can be held fully financially liable. The Port Authority will have to pay for all of the hundreds of millions in third party claims.

On April 29, 2008, the appeal process denied all the Port Authority's post-trial motions, leaving the 2005 verdict intact. A five-judge panel of the state Supreme Court unanimously agreed with a lower court judge who also refused to set aside the jury's verdict that the Port Authority of New York and New Jersey was negligent and more than 50 percent liable.

The appeals court said what the jury decided was that "the acts of these terrorists, even while obviously odious in the extreme, were not a cause for the easy absolution of this defendant from its civil obligations."

The NY Supreme Court upheld the verdict by finding that “notice” of potential terrorist attacks was the appropriate standard to apply to facility owners and/or operators. The Court agreed that “notice” occurs when a defendant knew or “should have known” that a terrorist attack was possible. The Court also determined that “reasonable” mitigation steps may now include those that may have previously been considered “burdensome.”

The “should have known” and “reasonable” mitigation steps elements has forever changed the liability landscape in a terrorism related lawsuit. In the post 9/11 world, virtually any terrorist attack, electronic or otherwise, will surely be viewed by a jury as a “should have known” event. *(FindLaw: IN RE: World Trade Center Bombing Litigation)*

Terrorism / e-Terrorism and Resulting Liability Exposure

Unlike the majority of the financial risks organizations face today, liability for a terrorist act, even partial liability, can threaten the entire organization or enterprise.

Any entity that buys, uses, installs, maintains, integrates, deploys, designs, creates, manufactures, supplies, sells, distributes, advises on, or is otherwise involved in security or cyber-security related products, technologies or services in any way, whether for themselves or for others, does so at an extraordinary risk. As evidenced in the Port Authority case, it is now much more likely that juries will view terrorist acts as "reasonably foreseeable”.

Victims will attempt to recover damages from any entity seen as being potentially negligent in not preventing or mitigating the attack. All your related security and anti-terrorism products, services, assessments, studies, analysis, equipment, engineering, technologies, manufacturing, research, development, testing, policies, protocol, decisions, procedures, facilities and infrastructure will be intensely scrutinized.

Whether you supply to others, use or do it for yourself, the fact that a terrorist event actually took place must mean something did not work, was missing or was inadequate. Regardless, it would be very hard to convince a jury otherwise. You may find yourself on the top of the "blame" list regardless of how minor your actual involvement may have been.

Because of these potentially catastrophic liability exposures, owners, officers and/or management have a fiduciary responsibility to explore the very broad immunities, liability caps, affirmative defenses and other protections that could potentially be afforded to them under the SAFETY Act. It is critical to know if and how your organization can benefit from this Federal law enacted as a part of the Homeland Security Act of 2002.

The SAFETY Act

The SAFETY Act is a little known and often misunderstood piece of legislation that can protect an entity from the truly "enterprise threatening" liability they could face following a terrorist event. This liability can come from an attack on their own facilities or an attack on a third party where the defendant's products, technologies, advice, procedures or services were defeated or exploited. The Act's protection can apply to a physical attack on persons or property, or to acts of cyber terrorism that cause physical and/or financial harm.

The SAFETY Act was enacted by Congress as a part of the Homeland Security Act of 2002 (Public Law 107-296). 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 development, manufacture, deployment, use or commercialization of products, technologies, procedures, software, system integration, advice and/or services that could prevent or mitigate a terrorist attack.

The Act provides unprecedented and sweeping immunities, liability protections, liability dollar caps, affirmative defenses and other incentives for entities who use, supply, design, manufacture, provide or are otherwise involved in preventing, deterring, mitigating, responding to or recovering from a terrorism event.

SAFETY Act protections apply to a certified act of terrorism when the qualified or "Designated" product, service or technology was used, deployed or otherwise alleged to be involved. The Act's protections can apply to "hard" products as well as to services, procedures, integration of multiple anti-terror tactics, overall facility protection, software, advice, etc. The law applies to products and services provided to, or used by, either the government or civilian sector.

The two most significant liability protections that can be afforded under the SAFETY Act are either a cap on your liability, or total immunity from suits arising from a terrorist attack.

- *"Designation"* under the SAFETY Act provides a maximum Dollar cap on your liability as determined by the DHS.
- *"Certification"* under the Act allows the assertion of the "government contractor defense" (Boyle vs. UTC) in essence creating total immunity from suits alleging negligence arising out of some element, failure or omission in the approved procedures, products, technologies or services. The successful assertion of this defense eliminates all liability under Federal statute and the case is immediately dismissed.

The SAFETY Act does not require that an entity be a government entity or contractor or even have any government sales or other governmental involvement whatsoever to assert this defense. Under SAFETY Act, and for the first time, the government contactor defense can be applied to solely civilian / private sector sales. Other benefits under the SAFETY Act include:

- Exclusive jurisdiction in Federal court for all related suits;

- Punitive damage claims are barred;
- Non-compensatory damages are barred;
- Non-economic damages are barred unless the plaintiff was physically harmed. These damages include pain and suffering, mental anguish, loss of consortium etc;
- Pre-judgment interest is barred - Pre-judgment interest is interest on an award normally imposed by the court from the date of the event until the date the ultimate award is paid;
- A prohibition on joint and several liabilities for non-economic damages – The defendant cannot end up being the “Deep Pocket”. Only the percentage of the total claim amount attributed directly to the defendant’s negligence can be recovered;
- Credit for other plaintiff recoveries - The defendant’s total liability will be reduced for other compensation available to the claimants from collateral sources such as other defendants, insurance, settlements, etc.

SAFETY Act can help entities of all types and sizes from small municipalities, garage business startups, and schools all the way to Fortune 100 companies. An applicant can be an individual or an entity such as a corporation or LLC. The applicant can be a public, quasi-public or private concern or a combination such as an airport or port authority. A municipality, county or state government entity is just as eligible under SAFETY Act as is a large publicly traded corporation. The applicant does not have to be a US citizen, based in the US or sell anything to the US government to qualify.

The SAFETY Act is very broad in scope as to what terrorism related identification, prevention, response, mitigation or recovery could be protected under the law. It can include anything that is designed, developed, modified or procured for preventing, detecting, identifying, or deterring acts of terrorism, as well as responding to or limiting the harm such acts might otherwise cause.

The Act’s protection can apply to things provided or sold to others as well as to things bought, used or done for an applicant’s own facilities that can help protect people and property from terrorism, including network / IT protection. These measures do not have to be exclusively dedicated to anti-terrorism as long there is an anti-terrorism or terrorism response element. They can have multiple functions. Examples that have both terrorism and non-terrorism functions include access control systems, security, communication, evacuation or lockdown procedures, cameras, firewall software as well as a vast range of other "technologies". A product, technology or service does not have to be new or “high tech” to qualify.

The Act's criteria, application, evaluation and approval process apply equally to services and intellectual property such as software as they do to "hard" products. The event does not have to cause physical injury or property damage. A terrorist's breach of a SAFETY Act approved IT system firewall or other security software that results in a financial loss is also protected.

SAFETY Act benefits can be obtained by applying to the DHS for one’s own protection. The applicant does not have to be the manufacturer, developer or seller of the products, technologies

Get Into the Act™
SAFETY ACT CONSULTANTS
Phone: (202) 640-4000 - Toll Free (877) S ACT HELP
Fax: (202) 407-7054 - www.SAFETYACTCONSULTANTS.com

and/or services to benefit. In fact, the applicant does not have to sell anything at all. SAFETY Act can apply to things the applicant does for itself. As an example, the SAFETY Act's liability protections can apply to a school or university for its security, warning and evacuation procedures on campus or, to its research or instruction in the homeland security / anti-terrorism arena. The SAFETY Act can benefit almost all organizations.

You do not necessarily need to apply to be protected. The law grants automatic immunity to any entity that uses, buys or distributes products, technologies or services that are already SAFETY Act Designated by another party.

Cyber Terrorism and the SAFETY Act

The SAFETY Act can drastically reduce or eliminate the enterprise threatening liability exposure an organization will face if a cyber-terrorism event somehow involves their systems, networks, hardware, software, products, advice, procedures, people, services or facilities. In addition, those entities that provide IT security related goods or services to others will enjoy a significant marketing advantage and higher demand for any SAFETY Act approved products or services.

SAFETY Act protects against allegations that approved products, technologies, services or procedures failed, were inadequate or somehow did not identify, prevent, respond appropriately or help mitigate an e-terrorism act. Protections apply to lawsuits alleging bodily injury, property damage as well as other harm, including financial harm.

Works Cited

In RE: World Trade Center Bombing Litigation. (2004, Janunary 20). Retrieved November 25, 2010, from FindLaw: http://caselaw.findlaw.com/ny-supreme-court/1143026.html

McAfee Labs. (2010). *McAfee Threats Report: First Quarter 2010*. Retrieved November 25, 2010, from McAfee: http://www.mcafee.com/us/local_content/reports/2010q1_threats_report.pdf

Mills, E. (2010, November 17). *Symantec to Congress: Stuxnet is 'wake-up call'*. Retrieved November 25, 2010, from cnet News: http://news.cnet.com/8301-27080_3-20023124-245.html#ixzz16PLPBfra

About the Author

Bob Karl is the founder and Managing Partner at SAFETY Act Consultants. He has extensive experience in aerospace, insurance, terrorism financial impact mitigation, as well as being an advocate and expert on the SAFETY Act and its potential applications throughout all business sectors including cyber risks. Bob has over 25 years of experience in the insurance industry including fifteen years of experience with two top global insurance brokers specializing in aerospace, homeland security, terrorism liability mitigation and risk transfer.

...

SAFETY ACT CONSULTANTS
Phone: (202) 640-4000 - Toll Free (877) S ACT HELP
Fax: (202) 407-7054 - www.SAFETYACTCONSULTANTS.com