



Cyberterrorism and the Home User

*By Sarah Gordon,
Senior Research Fellow
Symantec Security Response*

INSIDE INSIDE

- › What it is?
- › How does this affect me?
- › What can I do to make my computer more secure?

Contents

Introduction3
What It is?4
How does this affect me?6
What can I do to make my computer more secure?6
Conclusion7

> **Introduction**

Over the last several years there has been a consistent increase in the use of the word “cyberterrorism” in the news. You’ve heard about cyberterrorism taskforces, and read about budgets for cyberterrorism defense. After the atrocities of September 11th, 2001, the topic has very much come to the forefront, even though the average computer user would be hard pressed to give a good definition of what cyberterrorism actually is. That’s not surprising, as even many computer security professionals are somewhat confused over the issue too.

As part of Symantec’s ongoing security research we have been looking in detail at this area and exploring the impact this issue is having on many different types of computer user. In this white paper, we will talk about what that research shows and what that means to a home user. Finally, we will examine some steps that you can take to limit the risk posed to your computer, not just by cyberterrorism but by hackers and virus writers as well.

> What It Is?

When people discuss the threat posed by cyberterrorism, one of the biggest problems encountered is that there are many different definitions of the term itself. If you ask ten people what cyberterrorism is, you are likely to get many different descriptions. In all of these descriptions, however, there is a common thread: the computer is firmly ensconced as the target of cyberterrorist attack.

While this way of looking at cyberterrorism is popular, there are several problems with it. The most important is that the computer as target is only one facet of a much larger problem – the many faces of terrorism itself. There are many definitions of terrorism. For instance, the United States Federal Bureau of Investigation (FBI) defines terrorism as “The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives”. The United States Department of Defense (DOD) defines terrorism using a slightly broader brush, calling it “the unlawful use of, or threatened use, of force or violence against individuals or property, to coerce and intimidate governments or societies, often to achieve political, religious or ideological objectives”. The United States Department of State (DOS) definition states that terrorism is “premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents”. Finally, the United Kingdom Terrorism Act 2001 defines the use, or threat of use of political, religious, or ideological causes with the intent to influence a government or intimidate the public as terrorism – if the act involves serious violence, damage to property, public health, etc.

These are just some of the definitions created by governments as part of an overall strategy to address terrorism, and while they vary, in each case, the definition is functionally relatively close. These definitions not only determine how the various countries and agencies view terrorism, they can be used to derive the “elements” of terrorism; that is, attributes which terrorist events have. These primary elements are:

- People: Which individual, local groups, are involved?
- Place: What locations are involved in the event?
- Method: What is the method used in the event?
- Tool: What tools, or items, are used to carry out the event?
- Target: What is the target of the event?
- Affiliation: How are group members affiliated (formally/informally)?
- Motivation: What is the objective of the event?
- Outcome. What are the desired, and actual, outcomes of the event?

Just about any terrorist event can be summed up using these eight different elements. But this is just the beginning. Each element carries its own level of complexity. For example, “place” may include where an event transpired, as well as where it was planned, or where funds were raised, etc. A “method” may include not only things like creating fear, but activities like recruiting or generating propaganda. Finally, each of these eight elements can be examined on many levels including the ideological, intellectual, and consequential.

Sound complicated? It is. As you might imagine, adding a computer into the mix complicates things even more. The place for the computer in this list is far further reaching than simply as a “target”; thus, the next step in evaluating the role of the computer in terrorism is to consider all of the possibilities that emerge when the computer is added to each element.

For example, consider the first element, “people”. While a computer cannot (yet) act as the sole perpetrator of a terrorist event, the computer can radically alter interpersonal interactions between people. Anonymization and desensitization can make recruiting easier, and virtual identities can influence group dynamics. Additionally, the Internet complicates the issues of national, subnational and international groupings.

The computer can aid the terrorist in many other ways as well. For example, covert channels can provide for messaging; the web provides a powerful information gathering tool and arena for identity theft; individuals and groups are no longer confined to meeting with like-minded individuals in their own countries... the possibilities are almost endless. However, this raft of possibilities does not mean that we are helpless against the threat of terrorism aided by computers. A great deal can be and is being done to reduce the risks that we are faced with.

As you can see, computers can play a huge role in any terrorist event, whether or not it takes place in the virtual world. This realization forces us to change radically our assessment of cyberterrorism risks. Corporations are treating computer security issues more seriously. The position of Chief Security Officer is becoming commonplace within corporate America, and security companies like Symantec are continuing to produce the best products in the world to help protect our computing infrastructure. And, home users are learning how they can help exercise diligence in using—and protecting—their home computers.

> **How does this affect Me?**

How does this affect you? The short answer is that it doesn't, at least not much! The longer answer comes back to the fact that the things that tend to protect your little patch of cyberspace from viruses, worms and hackers are exactly the same things that you need to do to protect yourself from "cyberterrorism", however you choose to define it. As a reminder, those good computing practices are outlined below (see "What Can I do..." below).

We all need to take the threat of terrorism that involves computers seriously. Symantec is committed to this work, and is working with both government and industry worldwide to help make the global computing infrastructure safe and secure. So, while you may see articles talking about the dangers, most of these probably won't impact you directly.

Perhaps one of the largest roles that you may play is reducing the risk of causing network outage unintentionally. For example, there have been instances of "Distributed Denial of Service" (DDoS) attacks on the network. In such an attack, the attacker gets lots of computers to overload one particular machine on the network. The attacker does this by installing a "Trojan horse" on many machines, allowing him to launch his attack. You can play a role in preventing this kind of attack by keeping your machine more secure.

> **What can I do to make my computer more secure?**

There are three primary areas in which you should secure your home computer. First, you want to make sure that the data on your machine is confidential. For example, you would not want someone looking through personal finances, which many users keep on their machines. Second, you want to make sure that someone doesn't change your data without you knowing it. Lastly, you want to make sure that your computer does not lose data – that is, that your data is available to you when you want it. These three facets of security, more properly known as "Confidentiality, Integrity, Availability" form the basis for securing your machine.

For the home user, there are three primary ways that one or more of these pillars of security can be compromised: viruses and worms, hackers, and "natural disasters" (like pouring a can of Jolt cola over your machine!). Fortunately, there are simple and effective ways in which you can protect yourself from each of these threats.

For viruses and worms, use an anti-virus software package; by use, we mean install one and keep it up to date! For users of Symantec's Antivirus, that is pretty straightforward as the product can be configured to do this for you automatically; if you use someone else's product, consult your vendor. It's hard not to overstress the importance of this: it's quick and easy and provides so much protection!

Hackers can be dealt with in a number of ways. First, if you're a home user, don't simply dial in to the Internet without considering that in many instances, not only can you see other computers, but people on those other computers can see you! Consider using a personal firewall (like Norton Personal Firewall), which blocks unauthorized access to your machine. Make sure that you're protected on all levels, by using integrated products like Norton Internet Security. That way, when you go online, you know that not only are you doing your best to protect your data, you are also helping prevent hackers from using your computer to attack someone else's!

Finally, make sure that you backup your important files and data. This step is so often overlooked that it's only noticed after things have gone wrong when it is too late. Consider how much time and energy you have spent configuring your computer and entering data into it. Isn't that worth spending a few minutes protecting?

> **Conclusion**

Although the issue of Cyberterrorism sounds daunting, it really does not change a great deal for the home user. Being responsible in the way we use our computers is simply that: being responsible. If you take care of your machine, this complex issue is very unlikely to affect your home computer use. Happy computing!

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934**

www.symantec.com

**For Product Information
In the U.S., call toll-free
800.745.6054.**

**Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.**