

The Canaudit Perspective

Volume 4, Issue 3
March 2003

Special points of interest:

- Cyber Terrorism: Hype or Reality?
- Canaudit UNIX Audit Guide
- Upcoming Events

Cyber Terrorism: Hype or Reality?

By Chad Parks
Technical Specialist
Canaudit, Inc.

The cyber terrorist threat has been dubbed many things, including Digital Pearl Harbor, Digital Armageddon, and Digital Waterloo to name a few. Whatever you want to call it, the threat of cyber terrorism is real; it does exist. More and more, I am reading articles in popular periodicals protesting the hype about cyber terrorism, pronouncing that cyber terrorist propaganda is caused by information security firms and the Bush administration in order to make money and advance political agendas. Cyber terrorism alone may not offer all the death and unbridled public fear that a conventional physical terrorist attack may provide; however, consider the ramifications of a carefully orchestrated cyber attack in conjunction with a physical terrorist attack. I do not need to specify examples of such scenarios; your imagination should suffice. The risk exists, and we would be foolish to ignore it just because skeptics believe the threat is overly exaggerated and is merely hype.

We were first introduced to the potential threat of cyber terrorism when the movie War Games was released in 1983. Matthew Broderick portrayed a young computer hacker who broke into the U.S. Government's defense system and nearly started World War III. Ever since, cyber terrorism has been a topic of hot discussion and debate. After the terrorist attacks in the US on September 11, 2001, the issues of terrorism and cyber terrorism were bona fide and brought to the forefront of political debates and media warnings. Following the attacks Americans had many questions to which they demanded answers to: How could such a thing happen on American soil? What is being done to prevent it from happening again? What other avenues of approach could terrorists take to attack the US? Cyber terrorism is undoubtedly one of those other avenues of approach that we need to be prepared for.

Some authors for popular publications believe that the excessive hype of cyber terrorism will lead corporate executives to dismiss cyber security as simply a buzzword that will eventually pass like the Y2K paranoia did in the first week of January 2000. This argument is based on the assumption that corporate executives are ill informed and afraid of being viewed as paranoid by the shareholder, the workforce, and the media. Maybe they are; I do not know for certain what goes through the heads of corporate

executives. Some may believe if they ignore the problem, it will go away. Others may not even be aware of the threat or even feel their organization is at risk. For example, why would terrorists want to use a grocery store network or a retail office supply chain network to launch an attack? How could they successfully do it? It is the job of IT Audit and IT Security, and in part, the whole organization, to inform senior executives of the risks of cyber terrorism as they apply to their organizations, and to provide well thought out options to senior management to implement the fixes and controls required to protect corporate assets and customers from such attacks.

Some argue that there is no real danger of a cyber terrorist attack that could kill and or cause massive destruction. Nuclear launch systems, US intelligence systems, energy management systems, and air traffic control systems are all, allegedly, on isolated networks that do not connect to the Internet nor have any modems or wireless access points installed. These same people argue that these systems are so specialized that it will be extremely difficult, if not impossible, for an attacker to be able to take control of these systems much less gain access to a machine or network, and use it in a way that could hurt or kill people. Cyber terrorist skeptics speculate that a successful attack on these systems would require insider knowledge, such as that of a product developer. Let us take the blinders off for a moment. Potential cyber terrorist attacks are not necessarily going to be directed at critical infrastructure or government agencies. Consider what would happen if an attacker were to break into the systems that control how much potassium is put into daily vitamins. I am not a doctor, but from what I understand, too much potassium can be lethal, as can many other ingredients found in vitamins and other products. Of course, the attacker would also have to gain control of the system that conducts quality control as well. Now, what if the cyber terrorists where able to do this or a similar type of attack against several hundreds of common products at the same time? Dog food, cereal, baby food? Would terrorist organizations have accomplished their goal of inflicting massive casualties and instilling intense fear in the American public? Would this fear result in loss of confidence in our government and inflict severe damage to our economy? I am not sure; nobody can be one hundred percent sure. However, we do not have to sit by and passively wait for cyber terrorism to occur.

The benefits of taking measures to assess information security risks and implementing the required controls responsibly, in a timely manner, are twofold. Not only will corporations be protecting themselves from being used as a medium to conduct cyber terrorism, but they will also be protecting themselves from hackers, crackers, viruses, worms, and industrial espionage. In 2001, malicious hackers, crackers, viruses, and worms from around the world caused an estimated fifteen billion dollars in damage to the global economy. The devastation will predictably skyrocket in subsequent years. Hackers have no boundaries or borders, nor do cyber terrorists. Just as important as controlling the risk of cyber terrorism, is controlling the risk of poor cyber security. Fortunately, the same controls used to stop hackers will simultaneously reduce the threat of cyber terrorism. A cyber terrorist, simply put, is nothing more than a hacker or cracker working for an organized terrorist group with the same or similar goals as a conventional terrorist. By stopping one, we will, in essence, be stopping the other.

When we were approaching Y2K, also known as the "end of the world," the federal government required that all public companies disclose to their share holders what measures had been taken to prevent predicted disruptions and failures in their systems resulting from the year change to 2000. I feel the Bush administration should implement information security regulations along those same lines. By disclosing the fact that most large organizations --spend more money on the company coffee fund than cyber security-- (Richard Clarke, Special Advisor to the President for Cyber Security), investors would surely force a change in the trend. Once an organization has become targeted and successfully penetrated, I guarantee the issue of cyber security will be more important than coffee. It is time to change the "it will never happen to me" attitude to "what can be done to protect myself?" By researching the answer to this question, you may find that the best resolution may not cost as much as you had thought. We must learn to crawl before we can learn to walk. The same holds true for cyber security. Consider securing and protecting your legacy systems using the free vendor-supplied patches and fixes instead of replacing them with new state-of-the-art systems and spending millions on IDS and security solutions. Basic house keeping will take you a long way in defending against cyber terrorists and criminals, and will provide a solid foundation for developing better enterprise-wide information security solutions and practices in the future. If you cannot secure a critical legacy system without risking production failures,

consider working to protect the system from the internal network until a better solution can be reached, by using a firewall to isolate it from the rest of the network. It is easy to find reasons why something cannot be done. Organizations should step up to the sometimes difficult challenge of finding low-cost solutions to complicated problems such as cyber security involving legacy systems.

It is true that America has never suffered consequences of a true cyber terrorist attack, yet. On September 10, 2001, it was also true that no organized terrorist group had ever hijacked four airplanes, crashed two into the World Trade Center, one into the Pentagon, and one in a field in Pennsylvania, killing over three thousand Americans. I am not saying that we should live and work in fear of cyber terrorism, or even terrorism for that matter. In fact, I refuse to live my life in fear of terrorism, either cyber or conventional, as have many Americans. However, we all need to do our part to educate our organizations and ourselves about the risks of cyber terrorism, and need to take preemptive measures to prevent this sort of attack to the best of our abilities. In my three years of experience in penetration testing, I have noticed that it has gotten much more difficult to gain access to internal networks from the Internet than it was when I started this line of work. However, once inside the network, it is easier than ever to gain control of servers; domain controllers; database information; and confidential product, employee, and customer information. I propose that we continue the security momentum by bringing more of the effort inside and apply it to the internal systems, the systems that are the backbones of many organizations. Many organizations have already started this shift in momentum. Do not get left behind; remember, low hanging fruit is almost always the first to get picked.

As always, the comments and opinions in this article are mine and mine only. I invite you to email me your remarks and promise to respond personally to all of them.

Chad Parks / Technical Specialist, Canaudit, Inc.

2003 Canaudit, Inc.

Chad Parks is a Technical Audit Specialist with Canaudit. He is highly regarded for the techniques he has developed to penetrate modems and remote connection devices. He has also written several articles on the topic of computer security which have been widely published. Chad can be contacted at chad@canaudit.com.

UPCOMING EVENTS

Professional Development Seminars

Build your technical audit skills and keep up-to-date by attending any of our upcoming 2-day or 5-day professional development workshops. Our instructors excel in explaining new techniques in terms participants can easily understand.

At Canaudit, we believe in the control self-assessment process. Therefore, most of our auditing courses contain a complete set of COSO-compliant checklists.

Professional Development Week

******Last Chance to Register by the Early Registration Deadline and Save up to \$150******

Washington, DC area: (Early Registration Deadline – March 7, 2003)

Control & Security of Oracle - April 14-15, 2003

Control & Security of UNIX - April 14-15, 2003

I.S. Auditing: The First Step - April 14-15, 2003

Understanding & Preventing Electronic Fraud - April 16-17, 2003

Control & Security of PeopleSoft - April 16-17, 2003

The Ultimate Network Penetration Class

- Los Angeles, CA area – June 2-6, 2003 (Early Registration Deadline – April 25, 2003)

For more information, a course outline or to register, please visit our website, canaudit.com or call (805) 583-3723.

Canaudit UNIX Audit Guide

Audits are a necessary process in the business world, but they don't have to be labor intensive. In the past, auditors and clients have wasted a great deal of time playing questions and answers – the auditor asks the question; the client answers. This process assists the auditor in gaining an understanding of the business function. The process permits the auditor to create audit documentation and to analyze the control structure. Now, with the cooperative audit approach, we can optimize this once labor-intensive process. The auditor creates a series of forms and checklists and sends them to the client, well ahead of the scheduled audit date. The client completes the checklists, assembles the documentation, and sends it to the auditor for review. The auditor reviews the material and then visits the client to perform supplemental work and complete the audit.

This approach has several advantages. The first is that the business unit being audited

is not disrupted by the audit. They can complete the forms and checklists over a short period of time, at their convenience. In addition, as the client reviews the material, the client may choose to implement some controls before the actual audit commences. This results in a stronger structure of internal control and moves the benefits forward. Clearly, the cooperative audit approach is more supportive, less time consuming, and enables all concerned to focus on improving the business.

Last month we provided you with our Network Audit & Security checklists which many of you downloaded and have now asked for more. (This checklist is still available until April 1, 2003 at <http://www.canaudit.com/FTPRoot/Guide.pdf>.) This month I am including our UNIX Audit Guide which will also be available on the Canaudit web site until April 1, 2003. (<http://www.canaudit.com/FTPRoot/Guide.pdf>) After downloading the checklist file, email Gloriana@Canaudit.com, provide your name, address, phone and email address and Gloriana will send you the password to decrypt it. (You may forward this article to your associates so that they can download the Canaudit UNIX Audit Guide and register as well.)

Canaudit, Inc.

P.O. Box 2110
Simi Valley, CA 93062

Phone: (805) 583-3723
Fax: (805) 582-2676

Audits:

Email: gordon@canaudit.com
Email: chris@canaudit.com

Seminars:

Email: kristie@canaudit.com