

Managerial Guide for Handling Cyber-Terrorism and Information Warfare

Book Questions

1. *What is cyber terrorism and information warfare about?*

Cyber terrorism is the premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets. It is essentially the use of cyber space for the communication and coordination of terrorist activities, the gathering of intelligence of potential targets, a force multiplier for physical attacks by disabling emergency response systems, and for causing physical harm by electronically attacking control systems for dams, electrical systems, medical databases, and a host of other computer dependent infrastructures. Information warfare is defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy loses. The main distinction between these definitions is that cyber terrorism is about causing fear and harm to anyone in the vicinity (i.e. bystanders) while information warfare has a defined target in a war (ideological or declared).

2. *Are terrorists really that skilled?*

The new emerging form of terrorism uses asymmetric warfare. Threats to information systems are outside conventional warfare. Groups like al Qaeda are learning organizations that have shown their ability to use our own technology against us. They have also shown a long-term planning and preparation approach to their attacks. Many of their leadership are from middle class or better families. These people are neither ignorant nor stupid. Remember, the leaders of the September 11th attacks went to Western universities and received masters degrees in a host of technical areas

3. *Just how serious is the threat of cyber terrorism?*

So much of our livelihoods now depend on the secure use of computers for communications, transportation, banking, medical, etc., and these systems have been penetrated by hackers, crackers and cyber criminals for quite some time. Imagine what would have happened if mobile phone service were disrupted just prior to a major chemical attack. Visualize having your blood type changed in a medical database before a major operation. Law enforcement is working to integrate their computer systems to provide better sharing of criminal and terrorist activities. In the past, people like Kevin Mitnik have demonstrated their ability to break into judicial and law enforcement systems and actually remove their criminal histories. Envision a cyber terrorist removing five people from a

watch list hours before they board a jetliner. Imagine having your identity stolen and used to commit a terrorist act.

4. *What are the most common attacks on computer systems?*

According to the CSI / FBI 2003 Computer Crime and Security Survey, it was reported that cyber attacks occurred by Viruses (82%), unauthorized access by insiders (45%), Denial of Service (42%), system penetrations (36%), sabotage (21%), telecom eavesdropping (6%), and active wiretapping (1%) of all participants. These percentages are based on 530 respondents in a diverse set of key industry sectors such as local, state, federal governments, transportation, telecom, utilities, medical, financial, legal, education, retail, manufacturing, and high-tech. These attacks occurred despite the fact that most of the respondents had security policies and mechanisms in place as part of their prevention and response plans. Just imagine the number of successful attacks that went unnoticed and/or unreported, and by entities that were not even part of the survey.

5. *What can be done about cyber terrorism?*

Security comes in three parts: protective systems such as the encryption of communications and data, mechanisms and supporting technologies; configuration and maintenance such as access controls, and proper and timely updates; and people involving policies and procedures for the proper use of systems, and general awareness and security reporting. All three must be considered to ensure your systems and networks are secured. This can be accomplished by establishing a strong security awareness program, establishing a comprehensive security policy, creating and implementing a comprehensive disaster recovery plan, implementing the latest security technologies, conducting regular security audits, and working with law enforcement when security breaches do occur.

6. *Are we at risk at home, and what can we do to secure our home computers?*

More and more of us are working from home or taking work home. We store lots of personal information on our computers that can be used to steal our identities, or to penetrate and/or attack connecting systems. There are a number of things that must be considered if we are going to truly secure our home systems. The physical location and protective mechanisms of the computer itself, Browser Security, Anti-Virus programs, Firewalls, E-mail Practices and Encryption, Remote Software Security, Staying Backed Up & Updated, Multiple Accounts with limited permissions and child proofing, Wireless Security, Encrypting Stored Data, and staying away from Shareware & Freeware are the primary items that need to be addressed. All of these and more are discussed in my other book in simple, easy to understand language.