Preface

Introduction

In 1988, Cliff Stoll published a remarkable book entitled the *Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage*. The book was a report on the project in which he was involved in the course of the previous couple of years. Starting with the discovery of a fraction of a dollar imbalance in some computer accounts and through hundreds of computers in many countries, Stoll traced a spy operating from West Germany. The objectives of the spy, which were partially accomplished, were to penetrate the most secret details of the American defense system. From the reading of this book, we gained two very powerful impressions.

- At that time, the United States and its Western Allies were completely unaware and, surprisingly, not willing to entertain the possibility that their enemies might penetrate their computer installations in search of confidential information. Only persistency of such people as Stoll raised their awareness of this fact. Take note that this lack of awareness is related to the year 1988 and before.
- Stoll was employed at the University of Berkley, California, as an astronomer. He was a good example of a very specific type of person, who could be described as a scientist/hippy. It was remarkable to notice how the search for an invisible hacker changed his mentality and his attitude towards life.
The awareness of the viability of the American military system to be attacked started to germinate. In the mid 1990s, the term information warfare became quite popular. Many studies were conducted and published. Most of them drummed for alarm, concluding that the United States was not ready for this new type of warfare. Perhaps the best summarization was in a report prepared in 1998 by the Center for Strategic and International Studies entitled “Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo.” Similar voices were on the rise in Western Europe.

Following the tragedies of the September 11, 2001 attacks on the World Trade Center and the Pentagon, the realm of security received considerable attention, and there was increased awareness among wider groups of contemporary society. Shortly thereafter, the U.S. Patriot Act was enacted. This legislation brought about wide sweeping changes to a host of existing laws resulting in the enhancement of domestic security against terrorism and additional powers of surveillance, investigation, and international money laundering. It also emphasized the need for information sharing in order to protect the critical infrastructures of telecommunications, energy, financial services, water, and transportation. But it was not only the U.S. that responded; most westernized countries passed similar legislations to address this growing threat. These acts have been met with quite a mixed reaction from contemporary society. The reaction of a significant portion of the population indicates deep confusion. On the one hand, they are worried about decreased security of living conditions, but on the other, they are against national governments introducing limitations on widely understood personal freedoms.

The fact that terrorists can strike us at work without warning and with decisive focus has had an enormous impact on how we plan our activities. The use of everyday technologies turned against us is a horrific image, especially when we are unwilling participants. In 1991, Dr. Stephen Sloan put terrorism and technology into a broader context in his article entitled “Technology & Terrorism: Privatizing Public Violence.” He stated that the erosion of state-centric politics and the emergence of non-state actors, which includes regional inter-governmental, transnational guerrilla, and terrorist groups, has changed the interaction landscape. He goes on to suggest that the line between terrorism and states is becoming increasingly blurred as sympathy by portions of a populace for political subgroups increases. This will further develop the union between state-organized terrorism and non-state terrorists, forming alliances of conveniences. Ten years later, we have witnessed this expectation in action. Within this context, technology will facilitate the communication and collaboration of these relationships. In 2002, in a statement to the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select
Committee on Intelligence, Lieutenant General Hayden, Director of the National Security Agency, stated, “The volume, variety, and velocity of human communication make our mission more difficult each day.” He went on to say, “We had to keep pace with a global telecommunications revolution, probably the most dramatic revolution in human communications since Gutenberg’s invention of movable type.” He also stated that al Qaeda need only harvest the products of the U.S. $3 trillion per year telecommunications industry to facilitate its activities in a globally instantaneous and encrypted manner.

Remember, it is not just terrorists that use technology to enact political agendas. It has been estimated that over 30 nations have developed the capacity to actively participate in cyberwarfare, including the United Kingdom, China, Russia, France, Israel, India, Brazil, and Iran. Countries are developing cyber strategies to effect early warning systems and other information flows. These capacities, when combined with independent terrorist organizations, pose a considerable threat to all nations and their citizens.

Information technology has become a critical component in defending against terrorism by accessing the intelligence of potential actors and their activities. However, as a result, it has also become a key point of attack. A key component in homeland security (anyone’s homeland) is the protection of the critical information infrastructure. The inclusion of remote communication properties in electronics (i.e., alarm and environmental control systems, location identification of Global Positioning Systems [GPS] that can be used to route a vehicle in an emergency, and global Internet banking access) has implications for security and stability. Information technology increasingly is being integrated into military, civil, and business systems. As a result, cyberspace will become the next major battleground.

Cyber intruders continue to steal proprietary technical and commercial information. They have shown an ability to establish “back doors” into systems they have penetrated for later use in data retrieval and coordinated cyberattacks on bigger systems. The capacity to engage in such acts is relatively inexpensive and readily available to large numbers of individuals and groups. In the public domain, there are many proofs of these capabilities. There are groups of people whose life mission is to inform society about this (e.g., the group from California that calls itself The Cult of a Death Cow). The use of the Internet by terrorist groups is a growing concern by many experts. Is this hype, or are we seeing the emergence of a new terrorist attack form? It has been reported that al Qaeda uses the Internet for planning and coordination through the use of restricted accesses and encryption, recruitment of pro-Islamic hackers, and the measurement of potential infrastructure targets. In
addition, Shieikh Omar Bakri Muhammad, a London-based Islamic cleric, spoke publicly about al Qaeda’s plans to use the Internet for cyberattacks. Remember, several of the September 11th terrorists had master’s degrees granted by western countries. Terrorist groups are able and willing to acquire whatever skills that are required to accomplish their goals, and can do so within the borders of democratic, open countries. Later, these educated terrorists may then launch a series of coordinated attacks from within and without jurisdictional control of the intended targets as a pre-emptive or coordinated assault. Geographic isolation is no longer a reality with global networks.

In 1996, Bruce Schneier released his highly acclaimed book, *Applied Cryptography*, detailing the need and approach to utilizing cryptography to secure all digital transmissions. Some four years later, he wrote *Secrets & Lies*, in which he recants many of his original assertions that technology will solve our security needs. Technology alone cannot prevent attacks. He goes on to say that “what is required is detection and response,” and that “there are no technical solutions for social problems.” Therefore, all we can do is to make it as hard as possible for intruders and continuously improve our situation. This requires a pro-active approach that involves people, processes, and response procedures.

In the coming years, organizations will discover that protecting systems through redundancy alone is only effective if the foundational systems are secured. Otherwise, cascading events can cripple an organization’s capacity to perform its functions. The required security changes in business practices and policies are needed today to prepare for the future. Those that become a part of these changes will gain knowledge and experience, and ultimately will assist in guiding the direction that such measures will offer. It is in our own best interest in such changing times to direct our future operating environment through active participation. Communication networks only can be protected against attacks if all stakeholders participate. The multiplier effect can be effective for an economic infrastructure’s defense. We must protect ourselves and not rely solely on government. Securing our systems must come from a bottom-up process and not be delayed while we wait for a top-down initiative. The National Strategy to Secure Cyberspace, issued by the President’s Critical Infrastructure Protection Board in 2002, states that “government alone cannot secure cyberspace.” It requires individuals, businesses, governments, and educational institutions to jointly work towards this common goal. Plans must be established and enacted to respond to this global threat, not only at a governmental level, but throughout the private sector. Until new technologies are developed to combat cyberattacks, businesses must establish procedures and policies that harness their existing infrastructure. It is a business decision
that simply requires persistence. We as a community of individuals and business leaders must take aggressive action now.

In light of the synthesis of the world situation presented above, and in relation to the security of information systems, let us formulate the following observations.

- There is a growing interest in security issues and, in particular, information security issues.
- A rising wave of terrorist attacks against civilian targets and information systems has added a new dimension to information security issues.
- There is a considerable richness of publications about various aspects of information security, detailing this or that vulnerability and suggesting possible remedies.
- There are few publications, however, that explain to what extent information technology (IT) managers should include in their agenda issues related to the rising wave of the terrorists and cyber-terrorist attacks.

This book provides Information Technology (IT) managers with an understanding of cyber-terrorism and information warfare and how to handle the problems associated with them.

We would like to emphasize that this book examines security issues and recommends solutions from the point of view of typical Information Technology (IT) managers. It does not address security issues from the national or governmental point of view. There are, of course, frequent references to national policies or laws, but they are made within the context of an IT manager’s needs.

To provide this information, we divided the content of this book into three parts. The first part is a short introduction to information security. We believe that understanding the processes that laid the foundation of this discipline and led us through the years will help others assess current and future security issues. For the same reasons, we explain the roots of terrorism and how this planted the seeds of cyber-terrorism.

Cyber-terrorism and cyberwarfare have many faces. In the second part, we present the most probable forms of cyber-terrorism and cyberwarfare attacks. We define these attacks, describe how they work, and explain the most effective ways to combat them from the IT management point of view.
Many tools of the trade of cyberwarriors and cyber-terrorists are common. Therefore, limiting the book to the discussion of these attacks would be significantly incomplete for IT managers. For these reasons, we wrote part three of the book, which defines other security measures that may not be directly related to fighting cyber-terrorism, but can generally decrease an organization’s information vulnerabilities to any type of attack, including cyber-terrorists’ attacks.

In the epilogue of the book, we present our thoughts about the future of terrorism and cyber-terrorism.

This book is designed for IT professionals and IT managers, in particular. Hence, we took considerable effort to enhance our thoughts with the presentation of case studies, which explain in practical terms the points we are making. All the cases are real; either we have witnessed the stories ourselves, they were told to us by our friends, or we found them in literature. As many of these cases could be embarrassing to some people or organizations, we have hidden the relevant names or changed the stories somewhat without changing their merits.

Some parts of the text are framed. This is an indication of an especially important message we would like to pass on to our readers.

From time to time, when quoting some important statement or fact, we have inserted the reference directly into the text, but to smooth the reading process, we have decided not to reference every item we quote. Of course, we can provide detailed references if there would be a need. We understand, however, that some topics discussed in the book may raise the special interests of a reader. Therefore, after each chapter, we have provided a commented list of publications covering the issues raised in a given chapter.