Chapter 2
Economic, Political, and Social Threats in the Information Age

Eduardo Gelbstein
Webster University, Switzerland

Marcus Wuest
Deutsche Bank (London), UK

Stephen Fridakis
Food and Agriculture Organization (FAO), Rome, Italy

ABSTRACT

There does not appear to be a common framework for quantifying the impact of information security business disruption events resulting in the loss of availability, confidentiality and/or data integrity. Individual incidents are known to have had costs ranging from 1 million US dollars an hour to a bank loss of close of 6 billion Euro. Given the global nature of supply chains and electronic commerce, deliberate disruption through well conducted attacks could have devastating economic consequences. This chapter explores in some detail the various components of such consequences.

1. INTRODUCTION

Economic Jihad can take the following forms:

1. Financing the institution of Jihad and those who fight in Allah's cause.
2. Staging the economic boycott whose primary aim is to weaken the economy of the Zionists, the Crusaders and their allies, while at the same time, it strengthens the Arab and Islamic economy in a way that make it a self-dependent economy.
3. Destroying the economic interests of the enemy, using all possible means, like urging all workers and employees to stop dealing with enemies.

DOI: 10.4018/978-1-61520-831-9.ch002

Dr. Hussein Shihata, Professor of Islamic Economy at the Faculty of Commerce, al-Azhar University, Cairo, Egypt(2010)

Chapter 1 explored the dependencies that society has on ICT and here we shall explore the consequences of security breaches. While these may arise through many reasons, the focus is on breaches from deliberate and targeted attacks on systems, data and networks.

At the time of researching and writing this book (mid-2007 to mid 2009), the world was going through a major financial crisis that was not the result of an attack on information systems, but which highlighted the extent to which our activities are interlinked around the world.

A financial problem that originated in the United States of America spread quickly to the world's financial institutions, stock markets and ultimately their economies – in October, 2008 there appeared to be a real possibility that a number of countries could actually go bankrupt (Iceland, Hungary, Ukraine, Pakistan amongst them) and Zeeland did.

One of the lessons learned from this financial crisis was that many parties lost trust in the workings of the system and once this happened, politicians, financial experts, economists, journalists and anyone else involved could at best explain how the crisis started but not offer means to resolve it (at least not quickly).

It is certainly not impossible that a similar global chain reaction could be triggered by a well-executed attack under the banner of "Economic War", "Economic or Electronic Jihad" or any other that may have the capability of successfully defeating the electronic defenses of a high-impact and highly trusted organisation. Many calls for such actions have been posted on websites and, luckily, there has been no evidence that these actions are being carried out (yet).

If the explanation of how such a reaction started invoked the words "terrorism" or "war", we could expect a panic reaction of at least the same intensity as the financial market turmoil of 2008 that followed disclosures that various forms of derivatives were the equivalent of a house of cards and some investment firms a massive fraud.

2. CONSEQUENCES OF INFORMATION SECURITY INCIDENTS

The provision of information systems and technology services within an organization requires significant financial resources. The Gartner Group, a well established group that monitors the ICT industry, estimated that in 2008 the total volume of global business would reach $3.4 *trillion* - $1.98 trillion for telecommunications, $819 billion for services (outsourcing of operations and software development, consultancy and audit), $408 billion for hardware and $196 billion for software purchases (Tully et al, 2008).

These expenditures are made by public and private sector enterprises that, in addition, incur costs to operate and support ICT. There are many comparative metrics on how these expenditures vary between activities and sectors – percentage of total revenue, percentage of total expenditures. The author's preferred metric is Total Annual IT Expenditure per Employee and several IT industry observers and advisory services, such as Gartner Group publish such data every year.

In 1997, Paul Strassmann, in his book *The Squandered Computer*, gave figures ranging from a minimum of $580 to a maximum of $33,200 and argued that expenditure per employee did not have a strong correlation with business results (1997).

More recent and specific figures were published in 2006 by Revenue Ireland, comparing expenditure per employee in tax departments in different countries (Revenue – Irish Tax and Customs, n.d.). These range from €4,792 in New