Chapter 22
Can Total Quality Management Exist in Cyber Security:
Is It Present? Are We Safe?

Mahesh S. Raisinghani
Texas Woman's University, USA

ABSTRACT

This chapter examines the threats in cyber security. It identifies the risk of cyber attacks and argues the inability to defend against those threats in a cyber security program. The introduction provides a brief history of cyber security and how the information highway arrived at this point in cyber security. The first analysis examines the threats in cyber security in personal, private, and government computer systems. The second analysis examines the approaches to attacking those systems. The third analysis examines threats against private companies and government agencies. The final analysis examines major threats to cyber security.

INTRODUCTION

During the early years of the information highway, individual users were the major prey for viruses and Trojan attacks. Today, the favorite targets of interest are no longer personal computer users anymore but large organizations and even government agencies. The ease of access to the internet has increased the popularity and vulnerability of internet users. Increasingly skillful users are preying on unskillful users for personal and monetary gain. As personal and government agencies depend more and more on technology to successfully manage day to day activities, they are becoming more vulnerable to cyber threats and attacks. The types of threats can range from personal attacks from hackers, major environmental disasters, organized crime groups, foreign countries, and/or cyber terrorism groups.

With the increase in global terrorism in global markets, public agencies are becoming increasingly more vulnerable to cyber threats and attacks than any other time in history. The majority of these agencies have experienced some kind of virus, Trojan, or worm affecting the agency computer infrastructure. These events are burdensome and sometimes tragic to the infrastructure of the agency. When developing a cyber program in

DOI: 10.4018/978-1-4666-6324-4.ch022

any organization, one of the major tasks are to identify unknown threats in cyberspace. These agencies must take specific practical measures to prevent these types of risk from affecting the agency information sensitive and Personal Identifiable Information (PII). On October 3rd, 2011, President Obama declared October as "National Cyber security Awareness Month". This proclamation recognized the importance of the threat of cyber security and it is a reminder to us to remain vigilant in our abilities to fight cyber security with events and training to protect our personal and public information in cyberspace.

TOTAL QUALITY MANAGEMENT

Total Quality Management is an amalgamation of the philosophies of mainly 3 proponents namely W.Edwards Deming, Joseph Juran and Kaoru Ishikawa. The core philosophy of TQM believes that quality implementation was a process that involved all aspect of the organization, TQM also believed that implementing quality from the onset was cheaper than the alternative, believed that if employees wanted to give their best efforts and would do so if they were given the tools, that both senior management and rank and file employees needed to be involved in the quality implementation process.

Total Quality Management came into prominence in the 1980s as that era's term for the description of quality management programs and has become something of a social movement (Hackman & Wageman, 1995), and is currently prevalent in Information Technology, Education, Healthcare and Manufacturing Industries because these organizations realize the need for high quality production in order to compete favorable in their fields, Construction had yet to come to this realization and definitely need to if innovation and development are to be encouraged (Haupt & Whiteman, 2004) .

WHAT IS CYBER SECURITY?

Cyber Security is defined as the measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attacks (Webster Dictionary).

A Brief History of Cyber Security

We as humans have always wanted to process information quickly from merchants in a Chinese market in 1000 B.C. to economist today. The Chinese developed a way to account for large amounts of livestock at the local market during cramped spaces and time. The vendors needed quick and accurate tools to account for the livestock. "This led to the invention of the Abacus, the device many believe was the mother of the digital computer as we know it today, between 1000 B.C. and 500 B.C." (Kizza, 2003, p.2) During the 1800s and early 1900s numerous advancements were made in the design of the computer system. From early days of the Chinese to today, we have witness a rapid emergence of technology and a huge growth in computer systems. During the 1940s, 50s, and 60s companies such as IBM, Honeywell, and Control Data Corporation (CDC) were developing large mainframe computers to process large bits of information. In the sixties the development of the minicomputer, begin the age of the personal computer. The later part of sixties led to the development of large computers sharing more and more information. Later with the development of smaller computers engineers began developing less expensive and smaller computers designed for the individual users. The computers were still fairly expensive for the average household therefore only a select few could afford these computers. At the time companies that build computers did not begin to focus on individual use. It was not until the early seventies that the microprocessor was born. "A microprocessor is an integrated circuit with many transistors on a single board. Before the birth of the microprocessor, computer technology