Chapter 2
How to Educate to Build an Effective Cyber Resilient Society

Jorge Barbosa
Coimbra Polytechnic - ISEC, Coimbra, Portugal

ABSTRACT

The possibility that computers, in particular, personal computers, can be used for harmful actions affecting global computer systems as a whole, due to two main reasons: (1) hardware and / or software failures, which are caused by problems related to their manufacture which must be solved by their respective manufacturers and (2) failures due to actions or inactions of their users, in particular people with low computer skills, people of very low age groups, e.g. children, or very old age groups, e.g. ageing people, or others without a minimum of computer skills. This problem is aggravated by the continuous proliferation of equipment, namely mobile devices, IOT devices and others that have Internet connectivity, namely through a browser. There are the possible ways in the area of cyber education that can contribute to cyber resilience of society and these are developed in this work.

INTRODUCTION

Today's society, especially in the more developed countries, is almost entirely based on so-called information and knowledge technologies. Virtually all actions, both individual and collective, and both privately and institutionally, use in one way or another a computer in some of the processes they use in their daily lives and almost all of these computers are connected to the Internet.

Although these connection to the Internet has many advantages and it must be continued to use and develop its potential, like almost all human achievements, this use constitutes a double-edged sword. When used in its normal sense, it creates and brings enormous advantages to the daily lives of citizens and societies. The problem is when these potential and the objectives to be achieved are misused and used for actions contrary to the basic objective and that result in harmful actions for the whole society and its populations.

DOI: 10.4018/978-1-6684-3554-0.ch002

The possibility that computers, in particular personal computers, can be used for harmful actions has essentially been due to two main reasons: (1) hardware and / or software failures, which are caused by problems related to their manufacture and that must be solved by the respective manufacturers and (2) failures due to actions or inactions of their users, in particular people with low computer skills, people of very low age groups, e.g. children, or elderly-aged groups, e.g. ageing people, or others without a minimum knowledge of computer skills.

These people do not have a real and objective perception that computers can be used for harmful actions and the implications in the whole world information society.

This problem is aggravated by the continuous proliferation of equipment, namely mobile devices, IOT devices and others that have Internet connectivity through a browser.

As it is not very foreseeable that computers no longer have to give rise to computer failures that allow their use in these types of nefarious activities, the author is of the opinion that only a very profound change in the awareness of the population of these issues through massive cyber-education programs for safety applications to all age groups, professions and educational levels, that can be applied worldwide, can minimize this serious problem, thus creating, in the future, a more cyber-resilient society. The possible ways in the area of education that can contribute to this resilience are analyzed in this work.

CYBER ACTIONS AT PRESENT

Cyber actions of various types have increased annually in a dizzying way.

Many cybersecurity agencies and organizations, both governmental and private, that monitor this type of activity, have produced periodic reports all coinciding with the fact that the number of harmful cyber actions grow from year to year in a frightening way.

The actions reported refer to actions of common cyber-crime, more sophisticated actions targeting banking and financial institutions, actions to obtain personal data, namely personal banking and financial data, and even actions of cyber war or cyber espionage, such as military or industry, the latter seemingly unleashed by states or by organizations and individuals apparently connected to more obscure structures in some states.

One aspect that has also been emphasized in these reports is the sophistication of the attacks and the techniques used in them. This sophistication has been such that many of the software agents used are very hard to detect, and are often only detected when they are activated and trigger some of the actions for which they have been designed and "installed" in a sub-reciprocal way on the computers that make up the software network from which the computer attack will later be triggered. They are true stealth software agents that even technical computer users hardly ever detect, let alone most ordinary users who have only a minimum of computer knowledge and even so from the user's point of view.

The origin of these attacks has also diversified and the countries where they leave also have increased in number. However, this information may not be entirely correct given that one of the major problems is the identification and attribution of cyber-attacks. This results from the fact that most attacks come from botnet computers, which were in advance of actions for the software agents that will later be used in the attacks. As already mentioned, most of the time, its legitimate owners are totally unaware of the role that their equipment had or could have in these actions. It should be noted that most of the time users actively participate although unknowingly and innocently in the actions that allow them to install on their computers these agents of malicious software. Often these actions are motivated by the greed of