Chapter 10
Information Security as a Part of Curricula in Every Professional Domain, Not Just ICT's

Predrag Pale
University of Zagreb, Croatia

ABSTRACT

Information security is gaining attention of managers, leaders and public as attacks extend from "pure" IT systems into critical infrastructure which is being expanded to food production and supply, health systems, news media, educational resources etc. All parts of social, commercial and private life are under attack. In addition, new methods of attacks are appearing: slow san attacks and hibernated attacks. Thus, dedicated cyber defense forces are necessary. In addition, ICT specialists who design, deploy and maintain systems need appropriate education in information security in order for systems to be as secure as possible, in the first place. Also, white collar social engineers, domain specialists, are now able to perform highly sophisticated attacks. ICT specialists lack the domain knowledge to predict, detect and counter fight such attacks. This chapter shows why domain professionals need security awareness, education, readiness training and exercises, continuously.

INTRODUCTION

Information security is increasingly gaining attention of information and communication technology (ICT) specialists and system designers, but also of managers, leaders, mainstream media and broad public.

The understanding how much has the world become dependent of ICT and how much has ICT penetrated all aspects of our work and life is slowly dawning on all of us. The buzz about "Internet of things" (Ashton, 2009) (IoT, 2015) is raising awareness that not only people are users of Internet but rather on both sides of communication can be machines and devices without any role, interaction, interference or even awareness of humans, thus increasing the number of critical, important and vulnerable systems beyond any imagination and manageability with current competences, methods, systems and tools.

It is accompanied by raising awareness that this tags along important security vulnerabilities

DOI: 10.4018/978-1-4666-8793-6.ch010

and risks for large and important systems, national infrastructures and perhaps for the civilization as we know it.

However, full understanding of everybody's role in raising issues of information security and of their specific responsibilities and duties is still far away. As of today, in many national, multinational and global environments, it is not clear: who to call in case of a major cyber attack; who can and should actively work on protection; what about retaliation or preemptive strikes.

Actually, it seems that majority of mankind, especially the decision makers, neither fully understand the reasons for ever increasing number of attacks against information security nor have the concept of the domain that is in danger.

THE REASONS FOR INCREASED ATTACKS ON INFORMATION SECURITY

It is due to ICT's increased omnipresence and its importance in all aspects of private, industrial and social life in the first place, but it is also due to proliferation of a variety of attack tools and simplicity of their use. In the past only highly skilled ICT specialists were able to find and exploit a vulnerability of an information system. Today it is no longer true. Just anyone can download a tool from Internet and launch an attack with it against not only one, but potentially thousands of systems. Botnets, the networks of hundreds of thousands of compromised "ordinary" computers are being sold, even rented, as the platform from which to launch attacks (Botnet, 2015). The initial step of attack agent injection into the Internet can be performed from anonymous computers driving by

1. Unprotected wireless networks belonging to individuals, or
2. Institutions who are not-participating, or
3. Networks intended for public use.

Even protected networks can be broken in and used to launch an attack (Chatzisofroniou, 2015).

Perhaps the greatest problem with security of information systems and information security in general, globally, is in understanding the reason why would anyone wish to attack someone's computing and communication infrastructure and information they contain.

At the very beginning of general purpose computing and at the advent of Internet there were almost no security mechanisms and those in place were very simple (Symantec, 2009). Yet, there were almost no security issues, attacks and misuses.

The reason is in the culture of the users at that time. Majority of cyber community in 70-ies and 80-ties was situated in academia and the rest was in the government and military industry. The culture and code of conduct was well known to all members and was the core, essential to one's profession and identity. It was clear that any security breach in this community once detected would terminate one's career. Even worse, only the suspicion was sufficient to make one's life very difficult.

As Internet use spread to commercial, public and private areas, other cultures adopted it and inevitably brought their values (or lack thereof), attitudes and rules into the cyber world. Simultaneously, Internet was populated with information and resources of commercial, political and social value, making them interesting catch for those whose culture and code of conduct allowed to reach for them.

The general, western individualism and materialism significantly contributed to the raising issue of information security. The care for others, for local community and for society at large is heavily shadowed, if not completely erased, by huge appetite for possession, fame and personal experience and hedonism. Thus, anything others have that can help **me** to have more, be more and feel better is my potential catch and target. In the