Chapter 8.1
Future Trends in Digital Security

Daniel Viney
University of the Sunshine Coast, Australia

ABSTRACT

This chapter discusses ICT trends of the past decade, the emergence of Web 2.0 technologies, mobile computing (as distinguished from cloud computing), the pitfalls of social networking, security considerations in the workplace, copyright and Intellectual Property considerations, and how to best control threats and vulnerabilities. We are in a period of aggressive technological growth to which there is no foreseeable end. New technologies, such as Web 2.0 and cloud computing, are emerging at an exponential rate, and as a consequence, security threats, controls, and standards are iteratively evolving. As yet, we do not know the security and privacy implications that such a rapid and wide uptake of cloud computing, and other multi-user virtual environment initiatives, and Web 2.0 technologies, will bring. In no way is this cause to panic, instead it is cause to focus on self-education, employee-education, and awareness. To put it simply, these offer our best defense to security threats. By being educated, aware, and vigilant, the majority of threats are nullified, as they are designed to prey upon those who rely on trust when reading emails, visiting Websites, and accessing site content, when navigating the World Wide Web. For example, there are millions of users who are completely unaware of threats, such as phishing, and other forms of Internet-based fraud. More than ever before, the onus is on the individual, both at home and in the workplace, to be responsible for maintaining best practice techniques, while utilizing digital resources to ensure that information security, individual privacy, and applicable legislation are not breached. This can only be achieved through iterative education processes, general awareness, and vigilance.

DOI: 10.4018/978-1-61350-323-2.ch8.1

INTRODUCTION

Writing about the future is an ambitious undertaking, particularly with regard to technology. Gordon Moore, co-founder of the Intel Corporation, is one who has made an accurate prediction with a statement in 1965 that the number of transistors and resistors on a chip would double every two years (INTEL, 2005). This prediction concerning the future trends of computing capacity has become known as "Moore's Law" and a derivation of the statement, a common folk theorem, that the capacity of computing can be fitted to an exponential curve, with doubling time set close to a year and the dollar cost associated with that increase, decreasing along the same curve, is taught to Information Technology students the world over.

Whilst Moore (INTEL, 2005) was only discussing the humble computer chip, the accuracy of this prediction has seen technology become an integral part of our daily lives. There are few consumable products that one can buy these days, which do not contain a computer chip of some description. The ever decreasing cost, and ever increasing capacity of available technology, has seen rise to an almost unbelievable uptake in computing, within both the business and an individual's personal life over the past forty years, in particular the past decade.

Most of the westernized world is bordering upon having a dangerous level of technological dependence in their daily lives. If technology was to fail, as was widely feared by many in the build up to the new millennium, then we would see many businesses and essential services, including those of a financial nature and public transport infrastructure, devolve into complete disarray. However, such disruption is not only caused by a complete failure, or loss of service. For example, our uptake and dependence upon digital services, including: ecommerce, social networking, mobile computing, core business infrastructure, and cloud computing, has made us hugely vulnerable to an ever-increasing range of risks that could have immeasurable impact, should they occur. Consequently, we have borne witness to an evolution of digital security. Once upon a time, information security was less of a concern, bordering on being an afterthought; it was a cryptic discipline managed by mysterious individuals, who spoke a language that no one else understood. These days, information security is something that, although still not as widely understood as it should be, is at least a consideration of most people, be it the individual or the business. However, as computing continues to evolve and develop, so do the risks associated with it. As a consequence, digital security considerations are iteratively evolving and technologists simply must keep up.

So What is Digital Security?

First and foremost, we need to understand that the terms *information security* and *digital security* no longer simply refer to the task of keeping data concerning the business and its stakeholders confidential where appropriate, they also relate to ensuring the data stored has a high level of integrity, (that is - that it is accurate), and that the data is available and accessible upon demand. To grossly generalize: businesses need to maintain the privacy of their data to not only ensure that their core functions remain protected, that their product remains unique through protection of their intellectual property so that they can maintain a competitive edge; but also to ensure the privacy of their employees is maintained. These privacy factors include; biographical and demographic data, bank account numbers and transfer authorizations for financial institutions. Individuals also need to protect their own intellectual property, their financial data, and their privacy. In recent years, we have reached the scary realization that the onus is upon us all individually to be responsible for protecting our own identity. This is an amazing evolution that has thrown shades of ambiguity over something that we have all historically taken for granted.