Chapter 20
Trends in Information Security

Partha Chakraborty
Cognizant Technology Solutions, India

Krishnamurthy Raghuraman
Cognizant Technology Solutions, India

ABSTRACT

Information systems have transitioned from being designed for sophisticated users to systems for general populace. Have information security thoughts evolved likewise? The traditional understanding of security gravitated towards physical/network/platform/security and audit logging mechanisms. This chapter looks into evolution of information security, with the current impetus towards boundary-less enterprises, federated identities, the contemporary standards, and the need for federal governments to be involved in information security, ethics, and privacy concerns. With such a gamut of influencing forces, information security needs to be inbuilt with SDLC as a natural process rather than as an afterthought. This chapter covers information security trends in relation to cloud, mobile devices, and Bring Your Own Device. Convergence of information security with risk management and business process continuity is discussed. The authors indicate a few emerging research topics in the field of information security and outline the trends for future.

INTRODUCTION

Internet has enabled quick access of information transcending the limitations of time and geography. However, along with such convenience come grave risks: information on computers is more vulnerable to unauthorized access than information on printed papers. With physical papers, one can secure under lock and key. The ways of unauthorized access was limited. This is not true with information on computers. The silver lining is that the situation is not intractable: with the right application of techniques, tools and processes effective securing can be accomplished.

DOI: 10.4018/978-1-4666-3679-8.ch020

Though information security may mean different things to different people, one of the most succinct definitions is by the US Department of Defense (freedictionary.com, 2012):

The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

An often repeated theme in any definition of information security is 'protection' (Whitman & Mattord, 2012). Well established core principles of information security are: *C*onfidentiality, *I*ntegrity and *A*vailability (*CIA* triad). Authentication enforces Confidentiality; Authorization enforces Integrity; Non-repudiation help enforce Availability. Deep appreciation of the information security principles coupled with insights on changing social and technical landscape and the business drivers will help in formulating the most appropriate way to accomplish information security.

Due to widespread access of electronic information for a variety of purposes, *information security has emerged as an interdisciplinary subject* covering technology to sociology to political science. This is fueled by reliable and cheap internet connectivity for a significant portion of world's population. According to a statistic published by The World Bank in 2010, a little more than 30% of the world population is using internet. The channels of access and ways of offering information services are going through significant changes with the arrival of mobile devices, cloud computing and social media. Such novel ways introduce new challenges for information security: more users, different channels of access, possibility for abuse. One can imagine that the most secure system is the one to which no one connects. The business realities are just the opposite: enterprises of today are characterized hyper connections.

The aim of this chapter is to equip the reader with a reasonable sense of appreciation of current trends in the area of information security and the approaches to deal with the challenges emerging from the recent trends. The focus of the chapter will be on information security as applicable to the realm of applications and data. This chapter will analyze how information security is influenced by federal governments and will briefly look at the landscape of standards and regulations. The chapter ends with an outline of some of the research topics in the field of information security.

BACKGROUND

Computers, internet and information systems trace their origins to defense and research organizations. The seed thoughts about the usage possibilities were remotely related to business and mass populace. Systems were meant for highly educated computer geeks doing scientific or military tasks. This is not quite so now. Information systems permeate all aspects of life of an average person. However, information security thoughts remained rigid and did not evolve sufficiently fast to accommodate the new arrival of users who had no knowledge on the workings of a computer.

Computers and information systems have proved themselves to be a reliable part in our unending quest for efficient ways of accomplishing a task. Now our lives are inseparably bonded with information systems and it is no longer an option for us whether to have a digital identity or not. With such pervasiveness and reliance of information systems in our everyday lives, the concerns of privacy and national security have risen to such a magnitude that federal governments promulgate regulations on how to deal with digital information.

While, on one hand we see increasing reliance on information systems by the citizen, the businesses are continuously faced with pressures to innovate. Businesses are increasingly collaborating. Fresh ways to secure information – one that allows and encourages flow of ideas yet not compromise