Chapter 51
Identifying and Analyzing the Latent Cyber Threats in Developing Economies

Atul Bamrara
Indira Gandhi National Open University, India

ABSTRACT

Internet usage has increased significantly across developing economies in last decade and most of the enterprises are extensively reliable on computer networks for electronic mails to payment gateways. But, the scenario we live in today has become more and more connected, sophisticated and risk-prone to our network-delivered society. Nevertheless, it remains critical for enterprises to exploit the full potential of available technologies such as mobile computing, smart computing and cloud computing. A cyber security related gaffe in any of these rapidly emerging domains may lead to lost productivity and grave concerns to the enterprise. The chapter highlights the various concerns associated to cyber security, viz., how an attack may be operated and offered measures to secure the network and information technology resources within and outside the enterprise. In most of the developing economies no synchronized activities in this regard are taking place which opens the opportunity to cyber criminals intrude into the system and compromise the resources.

INTRODUCTION

Cybercrime is criminal activity performed using computers and the Internet. It also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting private business information on the Internet. Cybercrime is the latest and perhaps the most complicated problem in today's' world. Any criminal activity that uses a computer either as an instrumentally, target or a means for perpetuating further crimes come within the ambit of cybercrime. Symantec defines cybercrime as any crime that is committed using a computer or network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.

DOI: 10.4018/978-1-5225-5634-3.ch051

Industry, government and indeed society are becoming critically dependent on Information Technology (Anderson, 1994; Apt et al., 1997). This dependence is illustrated by the severe concerns which are now being caused by residual "Year 2000" bugs. Seeing that even these conceptually-simple software faults are demanding enormous resources, we must be concerned about the much more complex effects of "cybercrimes": malicious activities by "hackers" or organizations seeking to exploit or disrupt an IT system, for mischief, financial gain, or more sinister motives (Benjamin, 1990).

The footprints of cyber-threats across the developing world are getting superior. In the economies which are characterized by stumpy internet penetration rates and few resources devoted to combat cyber threats, formal institutions related to such crimes tend to be lean and dysfunctional. With the internet's rapid diffusion and the digitization of economic activities cyber-crime has gained momentum in developing economies. According to Kaspersky Labs, seven of the top ten countries for creating Trojans designed to steal passwords were developing countries, which accounted for 92% globally. Businesses and consumers in developing countries have also become victims of domestic as well as international cyber-attacks. Since most of the growth in the global PC market in the near future is likely to come from developing countries. A mounting number of cyber attackers are directing their attentions towards developing economies. The Philippines is one example of a developing nation that has been badly affected by cybercrime. Hackers from Japan, Malaysia, Korea, China and United States have targeted computers in the Philippines. The Canada based hackers controlled about one lakh poorly protected 'zombie' computers mostly in developing countries such as Brazil, Poland and Mexico stealing up to US$8 billion. Developing nations are also a becoming a safe place for cyber-criminal activities as most of the users in regions like Sub Saharan Africa and Southeast Asia gain Internet access. Online activities are not regulated or policed in these parts of the world, giving these criminals an advantage over their first-world counterparts.

REVIEW OF LITERATURE

In 2013, phishing alone resulted in $5.9 billion in losses to worldwide organizations, and three in four data breaches were attributed to monetary or fraud motives (Verizon, 2013). Cybercriminals have become more structured and adaptive, and continue to develop fraud as a service models which formulate some of the most innovative and advanced hazards and fraud technologies available to a much broader user base (RSA, 2014). Cyber threats are likely to affect everyone's routine activities today or tomorrow. Society depends profoundly on computer technology for more or less everything in life. Computer technology utilize ranges from individual consumer sales to processing billions of dollars in the banking and financial industries. The quick development of technology is also increasing dependency on computer systems. Now, computer criminals are using this amplified dependency as a significant opportunity to engage in illicit or delinquent behaviors. It is almost unfeasible to have precise statistics on the number of computer crime and the monetary losses to victims because computer crimes are hardly ever detected by victims or reported to authorities (Standler, 2002; World Bank, 2013, Pawlak, 2014). In addition, policing in cyberspace is too inadequate (Britz, 2004).

Moreover, the sophistication of computer criminal acts, by the criminals applying anonymous remailers, encryption devices, and accessing third party systems to commit a crime for the original target,