Chapter 4
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.

DOI: 10.4018/978-1-5225-1941-6.ch004

Copyright ©2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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.

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.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/identifying-and-analyzing-the-latent-cyber-threats-in-developing-economies/173128

Related Content

Biometrics: Past, Present and Future
Stewart T. Fleming (2003). *Current Security Management & Ethical Issues of Information Technology (pp. 111-132).*
www.irma-international.org/chapter/biometrics-past-present-future/7387

Enhanced Security for Electronic Health Care Information Using Obfuscation and RSA Algorithm in Cloud Computing
Pratiksha Gautam, Mohd. Dilshad Ansariand Surender Kumar Sharma (2019). *International Journal of Information Security and Privacy (pp. 59-69).*
www.irma-international.org/article/enhanced-security-for-electronic-health-care-information-using-obfuscation-and-rsa-algorithm-in-cloud-computing/218846

On Creating Digital Evidence in IP Networks With NetTrack
Diana Berbecaru (2018). *Handbook of Research on Network Forensics and Analysis Techniques (pp. 225-245).*
www.irma-international.org/chapter/on-creating-digital-evidence-in-ip-networks-with-nettrack/201613

Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would Share Their Password?
B. Dawn Medlin, Joseph A. Cazierand Daniel P. Foulk (2008). *International Journal of Information Security and Privacy (pp. 71-83).*
www.irma-international.org/article/analyzing-vulnerability-hospitals-social-engineering/2488

A Game Theoretic Approach to Optimize Identity Exposure in Pervasive Computing Environments
Feng W. Zhu, Sandra Carpenter, Wei Zhuand Matt Mutka (2010). *International Journal of Information Security and Privacy (pp. 1-20).*
www.irma-international.org/article/game-theoretic-approach-optimize-identity/50494