Global Cybersecurity: Issues and Concerns

By: Nir Kshetri

Kshetri, Nir (2013). "Global Cybersecurity: Issues and Concerns," Guest Editorial, *Journal of Global Information Technology Management* (JGITM), 16(4), 1-5.

Abstract:

By all accounts, the global cybercrime industry is significantly bigger than most of the major and well-known underground and underworld industries. The most often cited figure for the annual worldwide loss to cybercrime is US$1 trillion (Kshetri, 2013a). This is significantly bigger than the illegal drug industry and the human trafficking industry. According to the 2011 Norton Cybercrime Report released by Symantec, 69% of the world's internet users have been victimized at some points in their lives by cybercriminals.

Keywords: cybercrime | cybersecurity | social engineering

Article:

INTRODUCTION

By all accounts, the global cybercrime industry is significantly bigger than most of the major and well-known underground and underworld industries. The most often cited figure for the annual worldwide loss to cybercrime is US$1 trillion (Kshetri, 2013a). This is significantly bigger than the illegal drug industry and the human trafficking industry. According to the 2011 Norton Cybercrime Report released by Symantec, 69% of the world's internet users have been victimized at some points in their lives by cybercriminals.

There is a heightened sense of fear and anxiety about cybercrimes among individuals and businesses. According to a survey conducted by University of Calgary's Rozsa Centre, the average citizen is more likely to be a cybercrime victim than that of a physical crime. A survey conducted by IBM found that U.S. businesses worry more about cybercrimes than about physical crimes. An IBM survey released also found that there were three times more Americans who thought they would be victims of a computer crime "in the next year" than of a physical crime. A study conducted by *Gallup* in October 2009 indicated that 66% of U.S. adults were worried "frequently" or "occasionally" about being an identity theft victim.

An FBI report released in January 2006 indicated that the average attack cost around US$24,000, which included expenses related to repairing infected machines and networks and lost work time (Regan, 2006). Another study suggested that costs to repair virus-inflicted computers averaged US $81,000 per incident in 2002 (Roush, 2003). Firms that become cybercrime victims are also likely to lose customer trust and corporate credibility and may experience stock prices fall (Kshetri, 2006).

There are various sources of cyberthreats that individuals, businesses and government agencies face. A survey conducted among the members of the Confederation of British Industry indicated that the attackers in the most serious cybercrimes in 2000 were hackers (44.8%), former employees (13.4%), organized criminal groups (12.8%), current employees (11.5%), customers (7.9%), competitors (5.8%), political and protest groups (2.6%), and terrorists (1.4%). These threats translate into numerous types of predatory and market-based cybercrimes, which can be classified in terms of associated motivations of the criminals (extrinsic versus intrinsic), technology versus social engineering as the primary tool, jurisdiction of the targets (domestic versus international), opportunistic and targeted attacks and category of the targets and victims (individuals, businesses and governments) (Kshetri, 20l3a, c).

CYBERCRIME AND CYBERSECURITY ISSUES

This section highlights some of the major themes of this special issue.

Economics of Cybercrime and Cybersecurity

Prior literature has successfully applied economic theory to analyze individuals' cost-benefit calculus associated with engaging in cybercrimes (Kshetri, 2006) as well as conventional crimes (Becker, 1995). Prior researchers have suggested that from the potential victims' perspectives, an economic analysis can help explain the optimum investment necessary as well as the measures required to prevent hackers from cracking into their computer networks (Anderson and Schneier, 2006).

Cyberattacks Associated with Malicious Insiders

According to an FBI report from January 2006, over 40% of attacks came from inside an organization (Regan, 2006). In a high-profile case in this category, in 2001, two accountants at Cisco Systems pled guilty for breaking and accessing into unauthorized parts of the company's network and issuing themselves nearly US$ 8 million in company stock. Each was sentenced to 34 months in prison (Tedeschi, 2003). An analyst of the technology consulting firm Gartner estimated employees accounted for about 70% of computer system intrusions that resulted in a loss (Tedeschi, 2003). Likewise, a survey conducted among Irish businesses in 2007 indicated that about 40% of respondents said that internal cybercrime investigations led to firing or resignation of their employees (Madden, 2007). For these reasons, prior research has suggested the importance of background checks of employees (Kshetri, 20l3d).

Cyberattacks Involving Social Engineering

Cybercrime firms are found to combine a sophisticated mix of technical and social engineering competencies (Kshetri, 2013a, b). Among the many different ways of classifying cybercrimes, Gordon and Ford's (2006) categorization deserves mention. According to their classification, Type I cybercrime mostly contains technological elements while Type II cybercrimes have mainly human elements.

The basic idea behind social engineering is as follows: in many cases, it would be easier and more effective to trick potential victims to provide information than to steal it from them. Cybercriminals persuade potential victims with emotional appeals such as excitement or fear or establishing interpersonal relationships or create a feeling of trust and commitment. Social engineering has been an important part of modus operandi of a significant proportion of cybercriminals.

Importance of Trust and Trust-producing Mechanisms

Prior research suggests that in many industries, thin and dysfunctional institutions to perform trust-producing roles have hindered the growth of electronic market. Prior researchers have suggested that emergence of new intermediaries to provide services such as aggregating, matching suppliers and customers, providing trust, and providing inter-organizational market information would facilitate the growth of e-commerce market (Bailey & Bakos, 1997). In the search advertising industry, for instance, establishment of intermediaries to provide a third-party measurement system capable of producing trust could address some of the concerns related to click fraud.

Certification from auditing and professional organizations and other sources has been an important mechanism to produce trust in the digital world. For instance, The European Network and Information Security Agency (ENISA), the center of network and information security expertise for the EU, is expected to facilitate voluntary certification in the cloud. The ED has viewed that certification would make easier to signal and verify compliance and address cloud users' risk perceptions.

Articles in the Special Issue

This special issue has three papers that cover a number of research questions related to the above themes. In the first paper, Shu-Hua Chien, Ying-Hueih Chen and Jyh-Jeng Wu employ the two-step flow of communication theory to examine the contexts, mechanisms and processes associated with trust in driving consumers' intention to purchase online. The authors' analysis of data from 457 Taiwanese online shoppers indicated that third party issued e-certification and consumers' previous experience significantly affect trust on online vendors. The authors also found that the level of trust on a vendor significantly affects consumers' intention to purchase online.

In the second paper, Koteswara Ivaturi and Lech Janczewski analyze online security policies of banks from 11 countries in the Asia-Pacific region. The authors have employed content analysis to examine the banks' levels of preparedness to handle cyberattacks that primarily rely on social

engineering techniques. Their findings suggested that the security best practices of the banks mainly included preventive measures, and they were presented only as general tips and advices without sufficient details and situation-specific information. The authors conclude that such tips and advices that do not specify the context of a cyberattack are not an effective way of enhancing customers' cybersecurity orientation.

The importance of this topic stems from the fact that extrinsically or financially motivated hackers are likely to attack networks of companies with higher digitization of values (higher potential financial incentives) such as online casinos, banks, and ecommerce hubs (Kshetri, 2005). Cyberattacks relying on social engineering are even more prevalent in economies that have well-developed banking and financial sector. One example is Brazil, where cybercriminals reportedly use sophisticated social engineering scams to trick Brazilians into giving up personal information.

Regulators are gearing up to respond to this challenge. For instance, in 2011, the People's Bank of China (PBOC) issued a "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information". The "Notice", which has been effective on May 1, 2011, prohibits banks including foreign invested commercial banks, to store or process personal financial information obtained in China outside of the country. Likewise, the U.S. government requires commercial banks to secure their networks. To ensure the accuracy of financial data as required by Sarbanes-Oxley (SOX) compliance, IT controls need to be designed to ensure that data are accurate and are protected from unauthorized changes.

The third paper by Jian Hua and Sanjay Bapna proposes a game theoretical model that examines economic impacts of insider threats on businesses' IT security investments. The authors argue that malicious insiders are more dangerous external hackers and provide several examples of malicious insiders in a diverse range of organizations have been arrested and prosecuted. The authors came up with five propositions. With their mathematical and simulations the author conclude that optimal investment exists for the insider threat game. Their simulation results indicated that the optimal investment is a function of the attacker's advantage rate, breach function sensitivity and the deterrence level. They also find that organizations may need to invest more time and efforts protecting themselves from insiders than from external hackers.

CONCLUDING REMARKS

Global cybercrime is the biggest underworld industry of our times. Global forces and technologies such as mobile phones, social media and cloud computing are shaping the structure of this industry. Real and perceived threats of cybercrimes have led various problems such as quality uncertainty and risks, which have hindered the growth of global e-commerce. The three papers in this special issue have considered firms as well as consumers as the units of analysis in order to investigate cybercrime and cybersecurity issues that we face today. Taken together, they provide important insights into the challenges faced by organizations and individuals in the Information Age. They also present frameworks for calculating the appropriate levels of investments in cybersecurity and producing trust in the online environment, which would help develop a safer cyberspace.

REFERENCES

Anderson, R. and B. Schneier, 2005. "Economics of Information Security," *IEEE Security* & *Privacy,* (3:1), pp. 12-13.

Bailey, J, P., and Bakos, Y. 1997. "An exploratory study of the emerging role of electronic intermediaries". *International Journal of Electronic Commerce,* 1(3), 7-20.

Becker, G.S. "The Economics of Crime," *Cross Sections,* Fall 1995, pp. 8-15; www.richmondfed.org/publications/economicJesearch/the_economics_oCcrime/index.cfm.

Besler, P. (2005). Forced Labour and Human Trafficking: Estimating the Profits, working paper (Geneva, International Labour Office, 2005)

Gordon, S., and Ford, R. 2006. "On the definition and classification of cybercrime". *Journal in Computer Virology, 2,*13-20.

Kshetri, N. 2005. "Hacking the Odds," *Foreign Policy,* May/June, p. 93.

Kshetri, N. 2006.The Simple Economics of Cybercrimes", *IEEE Security and Privacy, January/February,* 4 (1), 33-39.

Kshetri, N. 2013a. *Cybercrime and Cybersecurity in the Global South,* Palgrave Macmillan: Houndmills, Basingstoke, U.K.,

Kshetri, N. 2013b. "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers," *Crime, Law and Social Change,* 60(1), pp 39-65

Kshetri, N. 2013c."Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations" *Electronic Commerce Research 13* (1): 41-69.

Madden, C. 2007. Firms trying to crack down on cyber-crime. *The Irish Times, 14.*

Regan, K. 2006. "FBI: Cybercrime Causes Financial Pain for Many Businesses," technewsworld.http://www.technewsworld.comlstory/4841 7.html. Accessed 1 October 2007

Roush, W. 2003. "The internet reborn: The internet has transformed the way we find information, shop, and do business. But it is a dumb network built for a bygone age. A university-industry coalition is designing a vastly smarter and more secure Internet: PlanetLab," Technology Review, 1 October 2003.

Tedeschi, B. 2003. "Crime is soaring in cyberspace, but many companies keep it quiet" *New York Times,* January 27, C.4.

Nir Kshetri, the guest editor for the special issue, *is Professor at The University of North Carolina-Greensboro and a research fellow at Kobe University. Among his*

four books are Cybercrime and Cybersecurity in the Global South (Palgrave 2013) and The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives (Springer-Verlag: 2010). Nir has published seventy articles in journals such as Foreign Policy, Journal of International Management, CACM, IEEE Computer, IEEE Security and Privacy, IEEE Software, Small Business Economics, Telecommunications Policy, Electronic Commerce Research and Applications.