



INDIAN INSTITUTE OF MANAGEMENT CALCUTTA

WORKING PAPER SERIES

WPS No. 600/ September 2007

Modelling Cybercrime for Internet Risk Management

by

Soumyo D. Moitra
sdmoitra@hotmail.com

Professor, IIM Calcutta, Diamond Harbour Road, Joka P.O., Kolkata 700104 India

Modelling Cybercrime for Internet Risk Management

Professor Soumyo D. Moitra
Indian Institute of Management Calcutta
Diamond Harbour Road, Joka
Kolkata 700 104
India.

sdmoitra@hotmail.com

Abstract: In this discussion paper we have considered the issue of cybercrime. This is now of considerable importance since the growth of E-commerce has increased the risks of various type of Internet crimes which we consider collectively here as cybercrime. It is argued that appropriate policy requires both better data on cybercrimes and more analysis of that data. The approach suggested here is to develop models of the cybercrime process and this will help identify the data needed more precisely. A basic modeling approach and its benefits are outlined.

Key words: Internet attacks, cybercrime, network security, risk management, E-commerce

Introduction

The growth and impact of the Internet has been widely documented. Along with these developments, the incidence and phenomenon of cybercrime has also been much discussed in the media, policy-making arenas and scholarly research. All this attention has resulted in the promulgation of a variety of computer-related laws and cyber laws in almost all countries. Not only national policy makers but regional blocks such as the EU as well as the UN have considered and implemented a number of measures to control cyber crime.

However, much of policy making is based on media reports, public reaction and ad-hoc data. Even now there is very little rigorous data collection that has been done and most of the surveys to date have serious methodological limitations. Thus there is very little reliable and relevant evidence of the extent and nature of cybercrime, and cyber laws developed in the absence of accurate data may not be really effective in practice. Similarly, organizational policies for protecting information systems that can be accessed over the Internet have been based on information and data that may be inaccurate and/or biased. The enormous growth of e-commerce has resulted in a very large number of organizations depending on the Internet to carry out essential transactions. Such organizations also need reliable data on cybercrime in order to manage the risks of being exposed to the Internet.

To develop effective policy to control cybercrime, it is essential that we have as accurate a picture as possible of this phenomenon. This requires, among other things, an

assessment of the current information on cybercrime since they influence the public and law makers. Such an assessment needs to appraise the survey methodology, the data and the analysis critically, identify possible biases in them and suggest better methods of data collection and analysis. Additionally, the available data (even if they were accurate) are far from sufficient for a proper understanding of cybercrime from a policy making standpoint. There are major gaps in our knowledge, such as the crime commission rate of malicious hackers, the relationship between cybercrime experienced at a site and the characteristics of that site or the detection and reporting rates of victim sites. Thus there is also a need for developing and fielding new questionnaires that could help us answer these questions. In order to develop such questionnaires, we need to develop models of the cybercrime process and consider the key variables that influence the incidence of the different types of cybercrime.

This is a discussion paper on the secondary data that is available and on models that might be developed that could help both Internet risk management and the design of future surveys. It is important that models are developed first to guide the empirical research so that more meaningful survey instruments can be constructed. Then we shall be able to collect data that would provide accurate insights into the cybercrime process and yield results that would be useful to further our knowledge of cybercrime. In the absence of appropriate models, we shall not know which variables are important to measure in order to assess cybercrime. Next we describe the methodology for some proposed research. Finally we note some of the benefits of the proposed research.

Data analysis and modeling issues

In recent years, a considerable number of reports have been published which present results of surveys or collected information on alleged cybercrimes. For example, the Computer Security Institute (Computer Security Institute 2006), the Bureau of Justice Statistics (BJS 2002; and planned for 2006-07), the Department of Trade and Industry (DTI 2006) and the Australian CERT (AusCERT 2006) have published reports that have attracted wide attention. Many other public and private organizations have also put out various kinds of reports related to cybercrime (noted in Moitra 2003, 2005c). While they have been widely publicized, very little critical re-analysis has been carried out on the reported data. Even less re-analysis has been done on any of the original data, since they are not made available. So paradoxically, on one hand they have been quite influential in policy making, yet on the other hand there are a number of potential biases and problems in the surveys and data collection (Wall 2005) which have not yet been adequately addressed. Clearly for effective and appropriate policies, the available data should be assessed and interpreted accurately, taking into account the possible biases (Moitra 2005c).

Thus, there are a number of outstanding needs in empirical cybercrime studies:

- Updated review of the standard available reports: CSI/FBI; AusCERT; DTI/PWC; {UK}; BJS/RAND
- Review of other available data {which requires a new search}
- A critical assessment of the methodologies and identification of potential biases
- Proposals to correct the biases and re-estimate the key results & interpret them
- Re-analysis/secondary analysis to the extent possible; that is, we should see what further light can be thrown on cybercrime from examination of these datasets/reports?
- Meta-analysis including trends analysis, now that we have several cybercrime reports, some over several years
- Literature review and theory development to the extent possible
- *The main issue is how can the current data be properly utilized to drive models of cybercrime and models for optimal security for organizations? What inputs can we derive for modeling?*
- There are two applications of this analysis: public cybercrime policy & private security policy for organizations. These need to be pursued.
- How should e-businesses develop their network security policies? The security policies will have many facets that need to be addressed: the type of security, that is, what type of information or computing or network assets should be emphasized; level of the security that should be put in place; the costs and effectiveness of alternative security systems; and finally we need a better characterization of a) information assets that are vulnerable to network attacks, and b) security systems or defense mechanisms.
- *Ultimately we need to know more about cybercriminals before we can develop EEE (effective, efficient and equitable) or optimal policies – whether public or private. This has to include motivations, active population size, skill level distribution, choice of MO (mode of operation), and crime commission rates – all by type of cybercrime. The challenge is to estimate these values from the very imperfect data that we have on cybercrime.*

We shall now discuss the methods and strategies to address these needs:

There are two sides to cybcrcrime and both have to be empirically analysed. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that the number of cybcrimes committed should be related to the number of victimizations experienced. Of course there will not be a one-to-one correspondence since

- a) one crime may inflict multiple victimizations
- b) multiple crimes may be responsible for a single victimization
- c) some crimes may not result in any victimization, or at least in any measurable or identifiable victimization

However, if we can develop ways to account for these diverse mappings between crimes and victimization, this reconciliation holds the key to understanding the incidence and impact of cybcrcrime. If in a given time period (say one year) N number of victims have experienced and average of v crimes, and A number of cybercriminals (attackers) have committed and average of λ crimes each then,

$$\lambda A = vN = C \text{ (= total number of cybercrimes)}$$

We can disaggregate the above by crime type (i) and then we have

$$\sum \lambda_i A_i = \sum v_i N_i = \sum C_i \text{ where } \sum \text{ represents the summation over } i.$$

And $A = \cup A_i$, $N = \cup N_i$ where \cup represents the union of the sets.

The above formulation is of course a gross oversimplification since many complications are being ignored. However, it represents a starting point and can be refined according to the needs of any particular analysis. For example, it may be important to factor in the complexities of cybercriminal behaviour such as the same person committing different crime types at different rates or the existence of group criminality. The estimation of victimization may be biased because (among other reasons) of non-reporting, incorrect reporting rates, non-detection of cybercrimes, etc. These and other complexities and extensions of this basic model have been studied in traditional criminology under the topic of criminal careers and victimization (Moitra 2003).

An example of a simple extension might be to take into account the average group size of criminals when they launch a network attack (say m_i) and the average number of victimizations caused by a single attack (say n_i) where both factors are disaggregated by crime type i . Then we have, as a first approximation,

$$\sum \lambda_i A_i / m_i = \sum n_i v_i N_i$$

The main thrust of this discussion paper is that we need to develop a sound empirical basis for the study of cybercrime. The currently available data has many shortfalls but in spite of that we can arrive at some tentative conclusions by making some reasonable assumptions and taking into account the possible biases in the available data. If we can proceed with estimating the above equations, then we will be able to take the first step to getting an accurate picture of the cybercrime process.

However, we need to go a step further and consider the impact of these cybercrimes. Unless we estimate the impacts of different types of cybercrime, we shall not be able to judge what measures would be most effective and efficient. Let \mathbf{d}_i be the average damage caused by crime type \mathbf{i} , then the total damage will be

$$\mathbf{D} = \sum \mathbf{d}_i \mathbf{v}_i \mathbf{N}_i.$$

But the term “average damage” may not be meaningful since even the same crime type may cause very different damages as well as different types of damage. Further the degree of damage inflicted will depend on the skill and resources of the offender. Finally, the damage will also depend on the level of systems security the victim has in place. Therefore we need more detailed models for the damages caused by cybercrimes.

There is also the very real issue of different network sites attracting different types of attacks and at different rates. A government site may attract hackers who ideologically oppose some policy or other; a financial institution will attract hackers who wish to break in to commit financial fraud, and a well-known company may attract intruders who wish to show off their skills by defacing their web-site. Other sites may be more anonymous and may hardly attract any cybercrimes.

A meaningful model will take all this into consideration. On the other hand, an overly detailed model could be cumbersome to analyse and perhaps impossible to estimate since its data requirements may be unrealistic.

Proposed Analysis

The data available in the above reports and which are relevant for policy analysis modeling has been identified and discussed (Moitra 2003). The next step is to develop a list of key variables and parameters that will be needed for modeling. Then we can develop a correspondence between what we have and what we need. This step will also reveal the information we do not have yet, and will lead us to a consideration of how such information might be obtained, if at all, and how we might proceed to collect it. Therefore, the following analysis is proposed.

- A systematic search has to be undertaken to identify additional data sets that promise to yield relevant and analyzable data. This would extend the MetaDataBase that has already been partially developed (Moitra 2003). This MDB lists the data sets in cybercrime that have data that can be used for research and policy analysis.
- Next, it will be necessary to consider models of cybercrime that conform to the current scholarly literature on cybercrime and which can be tested empirically. This will involve identifying the key variables that might explain the incidence of cybercrime and the patterns of victimization.
- The available data (in reports) need to be re-examined at this stage to what useful information may be extracted from them. It is possible and perhaps likely that with some plausible assumptions we can arrive at some useful estimates.
- Finally, given the need for better quality data in empirical research on cybercrime, we need to extend previous designs of survey instruments and develop questionnaires to collect data on the variable identified above. These would include i) the usage, experiences and attitudes of Internet users with respect to cybercrime; ii) the demographics the impact of cybercrime on organizations; and iii) the behaviour of hackers and cyber-offenders, if that would be possible some time in the future. The last is important because until we have some idea of the motivations, behaviour and activities of cyber-criminals, we shall always have a major gap in our knowledge of cybercrime.

Benefits

Here we summarize the potential benefits from the proposed research as discussed above.

- Better understanding of the current data on cybercrimes and the cybercrime rates for the different types of cybercrimes.
- Identification of inputs for modeling and simulating the cybercrime process. In turn, the models and simulation results could be utilized for more detailed policy analysis in the future.
- The results would be important for policy making since otherwise, there is the danger that policy will be developed based on incorrect notions and interpretations. Thus this proposed research should help in better surveys and these in turn will facilitate the development of effective, equitable and efficient polices for the control of cybercrime.

Bibliography

Adamski, A. Computer crime in Poland: three year's experience in enforcing the law. Available on the Internet. (www.sknpk.uni.torun.pl)

AusCERT. 2006. *The 2005 Australian Computer Crime and Security Survey*.

Baker, C.R. 2002. Crime, Fraud and Deceit on the Internet: Is there hyperreality in cyberspace? *Critical Perspectives on Accounting*, 13, 1-15.

BJS 2002. *Cybercrime against Business*. Bureau of Justice Statistics, Department of Justice, US.

Brenner, S.W. 2004. U.S. Cybercrime Law: Defining Offenses, *Information Systems Frontiers* 6:2, 115-132.

Caminada, M., R. van de Riet, A. van Zanten and L. van Doorn. 1998. Internet Security Incidents: A Survey within Dutch organizations. *Computers & Security*, 17, 5, 417-433.

CERT Polska. Raport 2003. Available at www.cert.pl/ .

Clifford, R.D. (Ed.) 2001. *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime*. Carolina Academic Press, Durham, NC.

Computer Security Institute. 2006. *The 2005 CSI/FBI Computer Crime and Security Survey*.

DTI. 2006. *Information Security Breaches Survey: Technical Report*. Department of Trade and Industry, UK.

Flanagan, A. 2005. The Law and Computer Crime: Reading the Script of Reform. *International Journal of Law and Information Technology*, 13, 1, 98-117.

Furnell, S. 2002. *Cybercrime: Vandalizing the Information Society*. Addison-Wesley, New York.

Goodman, M. 2001. Making computer crime count. *FBI Law Enforcement Bulletin*, 70(8), 10-15.

Grabosky, P., Smith, R.G. and Demsey, G. 2001. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press;

Hunter, R. 2002. *World without secrets*. Wiley, N.Y.

McQuade, S.C. 2005. *Understanding and Managing Cybercrime*. Allyn and Bacon.

- Moitra, S. D. 2003. *Analysis and Modelling of Cybercrime: Prospects and Potential*. Research in Brief/18, Max-Planck-Institute for Criminal Law, Freiburg.
- Moitra, S. D. 2005a. Internet Risk Assessment: Impact on Businesses. (IIMC WPS-570)
- Moitra, S. D. 2005b. Cyber Security Violations against Businesses: A Re-assessment of Survey Data. (IIMC WPS-571)
- Moitra, S. D. 2005c. Modelling and Simulation for Cybercrime Policy Analysis Research in Brief, Vol. 28. Max-Planck-Institute for Criminal Law, Freiburg.
- Moitra, S. D. 2005d. Developing Policies for Cybercrime: Some Empirical Issues. European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13/3, pp 435-464.
- NHTCU. 2004. *HI-TECH CRIME: The Impact on UK Business*. National Hi-Tech Crime Unit, UK.
- Newman, G. R. and Clarke, R.V. 2003. Superhighway Robbery: Preventing E-commerce Crime. Willan, Cullompton.
- Philippsohn, S. 2001. Trends in Cybercrime – An Overview of Current Financial Crimes on the Internet, Computers & Security, 20, 53-69.
- Suri, R.K. and Chhabra, T.N. 2003. *Cyber Crime*. Pentagon Press, New Delhi.
- Thomas, D. and Loader, B. D. 2000. *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge, London.
- Wall, D.S. (Ed.) 2003. *Cyberspace Crime*. Ashgate/Dartmouth.
- Wall, D.S. 2005. The Internet as a Conduit for Criminals - in Pattavina, A., *The Criminal Justice System and the Internet*, (77-98), Sage, Thousand Oaks, 2005.
- Westby, J. C. 2003. *International Guide to Combating Cybercrime*, American Bar Association, Chicago.