MAX PLANCK INSTITUTE
FOR FOREIGN AND INTERNATIONAL
CRIMINAL LAW

Managing Risk from Cybercrime: Internet Policy and Security Management for Organizations

SOUMYO D. MOITRA[1]

Contents:

[1] Indian Institute of Management Calcutta, Diamond Harbour Road, Joka, Kolkata 70010. India, sdmoitra@hotmail.com

Managing Risk from Cybercrime:
Internet policy and security management for organizations[2]

Introduction

The growth and impact of the Internet has been widely documented (Anandarajan, Teo and Simmers 2006, Barfield, Heiduk and Welfens 2003, Devezas, Linstone and Santos 2005). Most organizations use the Internet today in some way or other and the intensity of their use has been rapidly increasing (June 2005, Loomis and Taylor 2001, Macgregor and Vrazalic 2007).[3] The adoption of the Internet by individual users has also increased dramatically.[4] Along with these developments, the incidence and phenomenon of cybercrime has become a significant issue and has been much discussed in the media, policy-making arenas and scholarly research (Clifford 2001, Furnell 2002, Grabosky, Smith and Demsey 2001; Hunter 2002, Newman, and Clarke 2003, Power 2000, Taylor, et al. 2006, Thomas and Loader 2000, Wall 2007, Yount 2006). All this attention has resulted in the promulgation of a variety of computer-related laws and cyber laws in almost all countries (Brenner and Schwerha 2004, Broadhurst and Grabosky 2005, Koops and Brenner 2006, Suri and Chhabra 2003, Westby 2003).

---

[2] Some of this work was done when the author was visiting the Max-Planck-Institute for Criminal Law, Freiburg, Germany. The author would like to thank Prof. Hans-Joerg Albrecht, Director of the Institute, for his encouragement and support.

[3] Not only has the rate of growth in the usage of the Internet vastly exceeded those of the telephone and television, but the rate of improvement of the underlying technology, for example, as manifested by the speed of communications has also been bewilderingly fast. This has implications for both network security systems and the tactics of cyber offenders, in that there is an "arms race" in the techniques used by both sides.

[4] The number of host computers on the Internet was estimated to be at least 450 million in 2007, compared to less than 50 million in 1999, (www.isc.org, http//navigators.com). The number of users worldwide was estimated at 1.262 billion in 2007 following a growth rate of 250% since 2000. The penetration among the population was the highest for the US at 71% and the highest percentage of users came from Asia at 36.6% and the next highest was from Europe at 27.2% (www.internetworldstats.com). An idea of the size and the resources available on the Internet can be had from observing that Google has more than 3.08 billion pages and AltaVista over 1.7 billion pages. Altogether, the Internet has well over 17 billion pages of content. The growth in e-commerce in the US has been projected to grow from $115 to $329 billion in 2010 (U.S. Census and Forrester Research). Worldwide, over 183 million are estimated to buy online currently (IDC Research).

In fact, concern about cybercrime has been expressed in just about every conceivable fora: the media, the popular literature, researchers, various organizations, public officials and policy makers. As a result of all this publicity, there have been responses at all levels – local, regional, state, national, national clusters (such as the EU) and international. The US states were among the first to establish laws against computer-related crime which included cybercrime and now the US at the federal level, as well as most nations of the world, have legislation addressing cybercrime. The development of these cyberlaws has been extensively covered in the scholarly literature (Price and Verlust 2005, Samoriski 2002, Schell and Martin 2004, Spinello 2002, Yang and Hoffstadt 2006). The Council of Europe's *Convention on Cybercrime* was a major step by a group of countries to control the phenomenon and although many experts have identified problems with it and although there have been modifications and addendums to the original Convention, it is cited as a landmark in the area of cyber governance (Cangemi 2004, Flanagan 2005, Walden 2004).[5]

Not only national policy makers and regional blocks such as the EU, but international organizations including the United Nations have considered and implemented a number of measures to control cyber crime. This international response has taken many forms encompassing suggestions and guidelines to control cybercrime. Within the United Nations and its agencies a number of steps have been taken, for example, through UN GA resolutions 55/63, 56/121 and 57/239, among others (United Nations 2002, 2003). Resolution 56/121 is titled '*Combating the criminal misuse of information technologies*' and notes that while "the free flow of information can promote economic and social development, technological advancements have created new possibilities for criminal activities, in particular the criminal misuse of information technologies." It then "invites Member States to take" the measures set forth in resolution 55/63 into account in their efforts to combat the criminal misuse of information technologies. The resolution refers to the related plan of action against high-technology and computer-related crime of the UN Commission on Crime Prevention and Criminal Justice. The UN GA resolution 57/239 titled '*Creation of a global culture of cybersecurity*' notes that "as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all." It then exhorts member states "to develop throughout

[5] The policy-making is driven by the concern that, in view of the perceived risks in conducting transactions over the Internet because of cybercrime, the full benefits of the Internet to society are not being realized. These benefits include those arising from e-commerce as well as from a wider use of the Internet by the public globally.

their societies a culture of cybersecurity in the application and use of information technologies." The resolution also lists some elements needed for creating this global culture of cybersecurity.[6] UNCTAD in one of its reports (UNCTAD 2005) has emphasized that developing countries must take steps to fight cybercrime to benefit from the boom in e-business. Altogether, there is a clear awareness that cybercrime can be a major potential threat to achieving the promise of the Internet. As a result of this increasing international awareness, most countries have moved to put various computer-related laws and cyber laws in place, as mentioned above. In addition to enacting laws, there have of course been concurrent developments in law enforcement activities, (Broadhurst 2006, Clifford 2001, McQuade 2005, Sommer 2004).

However, much of the policy making is based on media reports, public reaction and inadequate data (Goodman 2001, Moitra 2003, Wall 2005). Even now there is very little rigorous data collection that has been done and most of the surveys to date have serious methodological limitations (Koellisch and Jaehnke 2006, Moitra 2005d). Thus there is very little reliable and relevant information of the extent and nature of cybercrime, and cyber laws developed in the absence of accurate data may not be really effective in practice. Indeed, we have no persuasive evidence to indicate that cyberlaws have had any substantial effect on the incidence of cybercrime.

We need to recognize that there are actually two realms of responses to cybercrime. One is that of public policy which seeks to control cybercrime for the good of society – local, national, regional or international. This activity is pursued (by almost universal consent) because policy makers at all levels feel that the wellbeing of all can be increased by having access to the Internet and its benefits. The citations from the UN documents clearly underline this feeling. In addition however, there is a second realm of response, and that is the response on the part of the users – especially organizational users since they have both a greater stake and greater resources in general than individual users. All organizations involved with e-commerce face risks from network attacks and cyber crimes because the Internet is an "open" network and almost anyone can get access. As a result, hackers and criminals can also access the computer systems and websites of organizations.[7] Thus,

---

[6] The United Nations has published a document titled "United Nations International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime."

[7] In response to these threats, many network security systems have been developed and there are now many network security firms that provide defense measures against network attacks. While both individuals and organizations are vulnerable, it is mostly the organizations

along with public cyber policy, organizations do and must take defensive measures against cybercrime.[8] But organizational policies for protecting information systems that can be accessed over the Internet have also been based on information and data that may be inaccurate and/or biased. As we have noted above, 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 properly manage the risks of being exposed to the Internet. Beyond getting good data, organizations have to have good decision-making methods to develop appropriate and cost-beneficial security measures. It is this issue that is the focus of this paper. However, there is a common need for an understanding of the cybercrime process for both public policy making and organizational decision making.

To develop effective cyber policy within both these realms, 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.[9] Such an assessment needs to review the survey methodology, the data and the analysis critically, identify possible biases in them and suggest better methods of data collection and analysis. These points have been addressed in prior work (Goodman 2001, Koellisch and Jaehnke 2006, Moitra 2003 and 2005d, Wall 2005) and it is expected that future surveys will provide a clearer picture of cybercrime patterns.[10] Thus there is substantial and continuing work on the analysis of cybercrime for policy development. On the other hand, while much discussion has taken place on how organizations should respond to cybercrime, and although there have been many developments in network security systems, there is relatively little work on how organizations should decide on the best kind and degree of security for themselves.

---

that have taken elaborate precautions against cybercrimes and cyber-attacks. Many have adopted various forms and levels of security measures to protect their networked systems and information assets. We refer to this as the private realm of decision making because these decisions do not affect public policy although some of the organizations may be governmental.

[8] For example, survey reports by the Computer Security Institute (CSI 2007), the Australian CERT (AusCERT 2007) the DTI, UK, (DTI 2006) tabulate various security measures organizations take and the incidence of network security breaches.

[9] Both the applications of the Internet and its underlying technology need to be taken into account, (Lessig 2000).

[10] One major effort has been the preliminary survey by the Bureau of Justice Statistics (BJS 2002) and a more comprehensive survey is currently underway. This survey has one of the more methodologically sound designs but even then there are significant limitations.

This paper addresses the problem of managing cyber security from an organizational point of view. The current organizational responses are also influenced by media reports, (though probably to a lesser extent than public policy), but it is strongly influenced by the marketing efforts of vendors of security products. Finally, it is also influenced by the various surveys of cybercrime (AusCERT 2007, CSI 2007, DTI 2006).[11] There are drawbacks to depending on such sources of information. Media reports should often be discounted because of the hype, and current survey reports are unsatisfactory as discussed above because of the numerous biases that exist. Vendors of security systems are naturally interested in selling more and expensive security solutions to organizations and tend to over-emphasize the risks. For a rational decision-making process, organizations need to consider the costs and benefits of network security measures comprehensively, and then deploy the system that is most appropriate for it.

In order to assess the costs and benefits of cyber security, it is obviously important to have accurate information about the prevalence and patterns of cybercrime. It is also important to derive an understanding of how cyber offenders behave and how they might respond to changing security levels. In this, both public cyber policy and private security decisions have a common need for more research and analysis of cybercrime. The focus of this paper is on the issue of how organizations can achieve the optimal type and level of security. This in itself is a complex task, as security has many dimensions that we shall discuss in detail. For now we shall note that there is this common need for information on cybercrime, and some of the modeling and analysis will also be relevant for cyber policy making. At another level, there have been calls for public/private partnerships for combating cybercrime (Grabosky, Smith and Demsey 2001, Wall 2003) although the extent to which it will occur remains to be seen. The point here is that both public and private organizations need the same information on cybercrime patterns for their own purposes. The situation is not too unlike that of the middle-ages when the king or emperor was supposed to maintain law and order in the entire realm, but in practice feudal lords and barons built their own castles for local protection.

In particular, this paper discusses data needs and specifically identifies the parameters needed for a better understanding of cybercrime. Further, it outlines an approach to estimate some of these parameters to the extent possible given the data that is, or potentially can be made, available.[12] The essential data that are needed

[11] Listings of many of these surveys can be found in Koellisch and Jaehnke 2006, and Moitra 2003.

[12] If researchers were given access to the actual survey data that have been collected by the various organizations rather than just the summary reports, we could do considerably more

are of two kinds: the first kind is the data related to cyber criminal behaviour such as individual crime rates, the number of active criminals and the choice processes by which they decide on committing crimes. The second kind is the data related to organizations such as the impact of cybercrimes on their network systems, the value of the information systems that are vulnerable and the costs of alternative security systems. This data can in theory be obtained and in fact should be known to each organization. The central uncertainty lies with the data regarding cybercrime and cyber criminals. Not having the level of detail and dependability in the data on the cybercrime process, we are not currently in a position to estimate the models we would ideally like to estimate.

In order to have a practical model for deciding on security, the model must obviously be estimable. The primary difficulty, as explained above, is that we have neither reliable nor sufficient data to estimate the models that would provide useful guidelines to organizations. In traditional criminology, many years of research and data collection provide a basis for the policy debates, but this is absent in the case of cybercrime. For example, in traditional criminology we have research results on victimization rates, individual arrest rates, self-reports from convicted offenders and studies on incapacitation and deterrence effects, and so on (Lersch 2004). Whatever their drawbacks, it has been possible to utilize the data for policy making to some extent. In the area of cybercrime, we have only partial and biased data on victimization, extremely little knowledge of cyber offender behaviour and no information on individual crime commission rates. The challenge therefore is to modify the models we would like to estimate. We need to make them simpler and more practical so that on one hand can be reasonably estimated and on the other hand are realistic enough for effective decision making. In this paper we first develop an initial model and then discuss the data we would need to estimate its parameters. Then we derive a simpler and more robust model that would still be useful and would be possible to estimate. We conclude with a summary and discussion that includes the potntial benefits of this work.

Model Development

First we introduce the terminology used in the model in Table I. A more detailed explanation of the notation is given in the model development below.

analysis and obtain a better picture of cybercrime. Thus, some of the required data exist but has not been made available so far for research.

Table I: Terminology

Symbol	***Name***	***Type***
λ	Individual crime commission rate	Variable
ν	Victimization rate of an individual organization	Variable
A	Number of active cyber criminals	Variable
N	Number of potential victim organizations	Variable
Λ	Total number of cybercrimes generated	Variable
V	Total number of victimizations	Variable
m	Average number of victims per cybercrime committed	Variable
μ	Average number of crimes that result in one victimization	Variable
g	Average group size of cyber criminals	Variable
r	Type of resource being protected from a network attack	Index
q	Level at which a resource is protected	Index
$\underline{\mathbf{s}}$	Matrix representing security measures taken [$\underline{\mathbf{s}} = \mathbf{s}(r,q)$]	Indicator
s	Scaled ordinal index to represent security level [derived from $\underline{\mathbf{s}}$]	Index
p	Probability of a crime by type of offender and type of victim	Variable
π	Transition probability to a particular damaged state | attack	Variable
Δ	Expected damage to a resource from a particular crime type	Variable
d	Damage per cybercrime experienced	Variable
D	Total damage per time period from a particular crime type	Variable
C	Cost of security by level	Variable
U	Utility to an offender from committing a cybercrime	Variable
α	Proportion of cyber criminals who are of a particular type	Fraction
ω	Proportion of organizations of a particular type	Fraction

i	Cybercrime type	Index
a	Type of cyber criminal	Index
k	Skill level of cyber criminal	Index
l	Organization type	Index
j	Damaged state after a network attack	Index
e	System-level entity that is the target of the attack	Index
θ	Mode of operation of the offender	Index

The initial model:

Let $\lambda = \lambda(a,k,i)$ = the rate at which a cyber criminal (or attacker) of type a with skill level k commits crime type i (that is, λ is the individual offending rate).

Let A(a,k) = number of active cyber criminals of type a and skill level l.

Total number of crimes committed of type i = $\Lambda(i) = \Sigma a\, \Sigma k\, A(a,k)\, \lambda(a,k,i)$

Let $\nu = \nu(l,\underline{\mathbf{s}},i)$ = the rate of victimization of crime type i experienced by an organization of type l with security level $\underline{\mathbf{s}}$. Here $\underline{\mathbf{s}} = \mathbf{s}(r,q)$ and is a matrix that reflects an organization's security position, with r representing the type of security (what resource is being protected, for example data or communications or resources) and q the level of protection.

Let $N(l,\underline{\mathbf{s}})$ = number of organizations of type l with security level $\underline{\mathbf{s}}$.

Total number of victimizations of type i = $V(i) = \Sigma l \Sigma_{\underline{\mathbf{s}}}\, N(l,\underline{\mathbf{s}})\, \nu(l,\underline{\mathbf{s}},i)$

If we make the 'zero-order' assumption that each crime will result in one victimization,

Then

$\Lambda(i) = V(i)$

However, in general this is not the case because a single crime can result in multiple victimizations and sometimes multiple crimes may result in just one victimization. For crimes of type i, let m(i) be the average number of victimizations per crime and $\mu(i)$ be the average number of crimes that result in a victimization.

Then

$\mu(i)\, V(i) = m(i)\Lambda(i)$

Or we can say that the effective aggregate crime rate is $V(i) = [m(i)/\, \mu(i)]\Lambda(i)$.

There is some evidence in the literature on hackers and cybercrime that cyber criminals often operate in groups, and that there may even be a division of labour among them in planning and carrying out an attack. If we wish to take group behaviour of the offenders into account, and if the average group size of offenders committing a crime type i is g(i), then,

$V(i) = [m(i)/\{g(i)\ \mu(i)\}]\ \Lambda(i)$.

In understanding patterns of cybercrime, it is important to understand the process by which criminals target victims. In fact we know very little about how cyber criminals and malicious hackers decide on which organization or organizations to attack.[13]

The choice will presumably depend on the type of offender, since almost by definition, different types will tend to choose different victims. Similarly, the skill level of the offender may influence the choice since potential offenders with low skill levels may avoid well-protected sites. Moreover, the choice will almost certainly depend on the type of organization, since different types of organizations will attract cybercrimes at different rates even from the same type of offender.[14] Finally, the choice may depend on the level of security the organization has for its resources that are vulnerable to network attacks. The targeting process itself may be one of several types: it can be totally random for example, or it may be based on the offender already having decided on the organization as a target, or it may be the culmination of prior network exploration and "sniffing" through which the offender has already gained some knowledge of the organization's network system. Whatever the details of the process, we shall observe a process where the nature of the crime, the offender and the victim are all significant variables.

From now on we shall employ a simpler form for denoting the organization's security posture (**s**). When all feasible combinations of security type (r) and corresponding levels (q) are enumerated, they will form a sequence of security levels and they can be ordered in terms of the degree of security they offer to the organization. Given complete market information, this sequence should also correspond to increasing cost. That is, the cost of a security system should be directly proportional to its effectiveness. If any system does not satisfy this condition, it should be dropped from the consideration set since it implies that there is some other system that provides the same or more security

---

[13] We are now ignoring the choice of individuals as targets as it is beyond the scope of this paper. However this issue needs to be taken up in the context of individual victimization and surveys of such victimization.

[14] This is assuming that offenders of a given type can commit different types of cybercrimes, possibly at different rates. If each type of offender specializes in just one type of crime then the choice problem is a little simpler.

for the same (or at a lesser) price. We shall represent any alternative in this ordered sequence by s, and so s is an index of the states of security that the organization can be in, with higher values indicating greater security. Let p(a,k,l,s|i) be the probability that an offender of type a and skill level k chooses a victim of type l with security s for committing crime type i. Similar approaches have been used in traditional criminology (Bernasco and Nieuwbeerta 2005).

We shall assume that $\Sigma l\, \Sigma s\, p(a,k,l,s|i) = 1$. That is, a given cyber criminal characterized by a and k will either choose a victim in each time period, or, if he does not launch an attack in that time period, we shall assign that null action to a dummy victim denoted by $l = 0$. Clearly λ will be a function of p and we shall develop this relationship later when we derive an expression for p in terms of a choice model for the offender's behaviour. We can also derive ν in terms of p as follows:

$$\nu(l,s,i) = \Sigma a\, \Sigma k\, A(a,k)\, p(a,k,l,s|i)$$

Turning now to the damage suffered by victim organizations, let the expected damage to resource r caused by an attack of type i be $\Delta(r|i,s)$, (dropping the indices a, k and l for now). The damage suffered from a crime of type i will be $d(i|s) = \Sigma r\, \Delta(r|i,s)$ taking into account all damaged resources, and total damage per unit time period will be $\mathbf{D(s)} = \Sigma i\, d(i|s)*\nu(i,s)$, since the rate of attacks is $\nu(i)$.

The d's will in general depend on the skill level k and the security level s. We shall consider the degraded state of the organization's system after the attack, which we shall denote by j. Then for each i, we shall have $\pi(j|k,i,s)$ which will be an element of a transition matrix that gives the probability of an attack of type i leading to a degraded state j given k and s.

Let $d_1(r|j)$ be the damage done if the end state is j, then

$$d(r|i,s) = \Sigma j\, d_1(r|j)\, \pi(j|k,i,s)\, f_3(k)$$

where $f_3(k)$ is the probability that the offender has skill level k, which can be taken as the fraction of cyber criminals with skill level k.

One issue we need to resolve is the effect of the organization's security level s since our central concern here is to identify the appropriate level of s. One paradigm that suggests itself is that λ is also affected by s, that is, the individual crime rate is influenced by the observed or known s (from experience or network reconnoitering). This implies that the security level acts as a deterrent, just as a secure facility deters break-ins in the physical world and this has indeed been suggested in the cybercrime literature (Grabosky, Smith and Demsey 2001). The alternative paradigm is that λ is exogenous with respect to organizational decisions and not influenced by s. In this latter case, s only influences

the damage caused (through π): higher levels of s result in lower damages (but the rate of network attacks remain constant with respect to s).

In this paper we wish to explore the first case which is more general, and we postulate a utility function for each offender that depends on s. Let U(a,k,l,s|i) be the utility to an offender of type a with skill level k if he commits a crime of type i against a site of type l with security level s. For now we shall simplify the notation by dropping the indices k and l and focus on just one crime type. Thus we have U(a,s) as the utility of committing this crime or attack. This approach follows from theories of crime that postulate a rational basis of crime commission (Becker, Tommasi and Ierulli 1995, Hellman and Alper 2006, Lersch 2004) and we shall return to this concept later.

Since the logit model for choice has been so successfully applied to many areas of individual behaviour involving choice (Train 1986), we shall use the logit model here. In our case we have a binary choice on the part of the offender – to commit a crime or not. By scaling the utilities such that the probability of not committing a crime has a utility of 0 (which we can do without any loss of generality), the logit model will predict the probability of an offender of type a committing the type of crime under consideration against an organization with security level s as

$$p(l,s) = \exp U(l,s)/\{1+\exp(U(l,s)\}$$

A major problem is that it will probably be extremely difficult to estimate the utilities. In theory, we can elicit the information necessary by interviewing cyber criminals or hackers, as has been done in some cases in traditional criminology, but most likely this will not be possible in the case of cybercrime. However, we shall see that for our purposes here, we do not need the utilities themselves, but rather their sensitivity with respect to the perceived security level s. In other words, if we can somehow infer how s influences the decision of these criminals to commit a crime against an organization that has a security level s, we can proceed to identify the most appropriate s for an organization.

Let $u(a,s) = \delta U(a,s)/\delta s$, the differential of U with respect to s.

We can assume that u(a,s) will depend on a very significantly as follows:

Let a = 1 for cyber criminals who commit crimes for financial gain. Therefore we can assume that they would prefer easy targets and their utilities decrease as s increases. That is, the differential or slope will be negative, that is, $u(1,s) < 0$.

Let a = 2 for cyber criminals who commit a crime for the sake of the intellectual challenge, and therefore their utilities will increase as s increases, since for them, the stakes and their reputation increase with s. Therefore the slope will be positive, or

$u(2,s) > 0$.

Finally, we shall let a = 3 for criminals who are ideologically motivated, that is, they wish to commit a crime against that organization for ideological (or emotional) reasons, and we shall assume that for these criminals their utility is independent of the security level and u(3,s) = 0 for all levels of s.[15]

If we can make some estimates of the u's from the cybercrime literature, particularly the literature on cyber criminals, then we can proceed with estimating this model and arriving at the best security levels for organizations. There are some reported findings in the literature that suggest that this may be feasible (Biggs 2004, Douglas 2002, Smith, Grabosky and Urbas 2004). Alternatively, if we can estimate $\delta p/\delta s$, that is how the probability of launching an attack may vary with the difficulty of carrying it out, (since the difficulty will be proportional to s), we can also estimate the model. This is because in our formulation (based on the logit model) there is a one-to-one relationship between the utilities and the probabilities of committing crimes.

Actually, what we need, strictly speaking, is $\delta v/\delta s$, and if we could somehow estimate this in aggregate (over all types of cyber offenders) then we could proceed with estimating the best level of security for an organization. However, in principle, if cyber offenders are non-homogeneous, and their response to the security level of potential targets vary by a and k, then, in order to accurately predict changes in victimization rates due to s, it is necessary to have some understanding of their utility functions and also the numbers of the different types of offenders [A(a)] that are active in a given period of time.

The decision problem for the organization is to minimize its costs (**C**) arising from the security measures it has installed and the total costs of damages (**D**) that it may still suffer from cyber attacks. This is because no security system is fool-proof and in spite of a security system, however good, some attacks and crimes will be successful and may inflict damages on the organization and its information systems. Thus,

The objective is to **minimize Z = D + C** with respect to s (Moitra 2007).

The solution will be at the point where

$\delta \mathbf{Z}/\delta s = 0$ or when

$\delta \mathbf{D}/\delta s = -\delta \mathbf{C}/\delta s$

The detailed derivation of the solution is given in the appendix. For simplicity we have dropped all the indices a, k, l and also i. That is, we focusing on one homogene-

[15] u(3,s) can of course be taken as less than 0 if that is what the evidence suggests. In any case, these three types of utility functions cover all possible responses with respect to security levels as far as the first order derivatives (u) of the utilities are concerned.

ous type of cyber offender, with all offenders of this type having the same skill level. Furthermore, we are concerned with a given organization now, so l is known and hence fixed. Finally, this simplification implies that we are now following one type of crime only.[16] What we have finally is that the optimal level of security (s) will satisfy the following equation:

$(\delta d/\delta s)^* \upsilon + d^*(T/N)^*[\{expU/(1+expU)^2\}^*(\delta U/\delta s)\}^*A\} + (\delta A/\delta s)^*p = -\delta \mathbf{C}/\delta s$

The procedure to solve this numerically is also described in the appendix. Here we discuss and interpret each of the terms in this equation.

The variables υ, d, s, T, N, U, A, p and C have been defined above in Table 1 and discussed in the text.

δd/δs = This is the change in the expected damage from a crime as the security level changes. This should be known to the organization. The systems managers should be able to estimate this as this is part of systems engineering. This is not to admit that it is difficult, but a good understanding of the alternative security systems and the organization's network/information assets at risk should provide the estimates. We have indicated an approach above.

δU/δs = This is the change in an offender's utility as the security level of the target organization changes. This is the most difficult term to estimate. Moreover, this strongly depends on the type of cyber criminal as has been discussed. It is possible that with further research on cyber criminal behaviour, we can arrive at some assessment of this, as has been attempted in traditional criminology (Bernasco and Nieuwbeerta 2005). Alternatively, we can also solve the model if we can estimate δp/δs in some way, as that might be easier, or if we can estimate δυ/δs in aggregate.

The latter may also be possible, even from current surveys, if the data collected in them were analyzed appropriately.

δA/δs = This is the change in the number of active cyber offenders who might consider this particular organization as its security level changes. This may be interpreted as capturing the deterrent effect of increased security. As its security increases, presumably few potential offenders will attempt to attack that organization.

---

[16] We can always re-introduce these indices. In that case, we shall have to sum up over the relevant indices every time. In the even more complicated scenario that there may be correlations among some variables, the interaction terms will have to be included. However, at this stage, the simplifications we have introduced appear reasonable, since we have no information to estimate a more detailed model. In fact, as we shall see, we shall have to make further simplifications and approximations to this model.

$\delta \mathbf{C}/\delta s$ = The change in the cost of security as the security level changes. As pointed out above, this should be known to the organization.

A Numerical Example

Next we introduce a numerical example to illustrate how this approach can be applied in practice (Moitra 2007). This example is simplified for expository purposes, but it shows how the model developed above can be used for arriving at security decisions. The only limiting factor in applying a fuller model is the availability of data.

The model itself is not exceptionally complicated – in fact, many real models that have been used by public and private organizations are far more complex – and the solution techniques are also quite straight-forward given the computer packages now available. Therefore, if an organization can gather the data needed for its own situation, it can easily apply a more comprehensive model that would be appropriate for it and arrive at the best security decision.

We consider three generic types of damage: damage to resources (computing and communications); damage to data; and damage to image or other intangible damages. These can be thought of as three types of assets any organization can have. We assume that the organization can estimate the total damage D in monetary units.

We also need to consider different types of cybercrimes. There are many ways of classifying cybercrimes (Moitra 2004) For example, we can consider

a) crimes with different goals: financial gain, show of skills, ideological;
b) crimes with different targets: information theft, sabotage, website defacement;
c) crimes by different types of cybercriminals, where type of cybercriminal would determine the crime type. This implicitly assumes that cybercriminals are specialists.

Whichever way we may choose to classify the crimes, in this paper we consider two types indexed by a (a = 1, 2). This is equivalent to assuming that cyber offenders are specialists and that an offender of type a commits only type a crimes (or, a = i, according to our previous notation. In addition to the crime type, we consider the skill level of the cyber criminal. We shall limit ourselves to two skill levels here: (k = 1 {low} or 2 {high}).

Finally we consider the types and levels of defense or security the organization can have:

We assume that different security systems are specialized to provide protection to different assets or resources. Although this is not strictly true and in practice a security system will provide protection for multiple resources, we make this assumption to capture the main impact of organizational decisions that may target a particular resource for protection. For example, an e-store may emphasize protection of its communications facilities, while a bank may be much more interested in protecting its data. As before, let **s**(r,q) represent the matrix that reflects an organization's security position, where r represents the type of security (what resource is being protected) (for example, r=1 {data} or 2 {communications}) and q the level of protection, (q=1 {low} or 2 {high}). We note that **s**(r,q) is a matrix with 0-1 elements, and only one element per row will be applicable for a given organization: that is, for each type of resource, the organization will choose either a low level or a high level of protection for it. We shall also need the corresponding cost data C(r,q) which gives the costs for each security system.

Next we consider the cybercriminals and the generation of cybercrimes. Let us assume that the rate of crimes committed will vary with the type of crime. Therefore,

Rate of crimes = arrival rate of 'incidents' $\Lambda = \Sigma_a \nu(a)$

where = $\nu(a)$ is the victimization rate for crime type a. We shall consider two types of crime for now and so,

$\Lambda = \nu(1) + \nu(2)$.

These crime rates may be estimated if we can compute the probabilities of committing each of these types of crime. Assuming that these probabilities are independent, they can be derived from the utilities of committing a given crime using the logistic choice model.

Let

U(a) = utility of committing a crime of type a (independent of k for now), and

U0 = utility of not attacking (assuming it is the same for all hackers, and U0 can be set to 0 without loss of generality).

Then, the probability of an individual committing a crime type a is

$p(a) = \exp(U(a))/[1+\exp(U(a)]$

based on the theory of utility maximization given a random utility model of choice (Train 1986). We shall take p(a) as the probability over a unit time period, which we assume as corresponding to the decision-making horizon of a cyber criminal.

To apply this model, we need data to estimate U = U(a | r,q) that is, estimate U as a function of type of crime as well as the type and level of security. This is reasonable since the utility will clearly vary by type of crime. It will also vary by the kind of protection the organization has installed, since this will affect the time and effort the cyber criminal will have to put in to commit the crime.

Then, the rate at which crimes are generated is given by

$\lambda(a) = p(a)^* T * A(a)$ and $\nu(a) = \lambda(a)/N$ if there are N organizations that are potential targets.[17] T is the time period and A(a) are the number of active criminals who would consider committing crime type a and whose utilities for committing that crime equal U(a). Thus $\nu(a)$ is the number of crimes of type a that the organization will experience. There is also the assumption that attacks follow a pattern of Bernoulli trials, so that the number of expected crimes by an individual offender of type a is p(a)*T.

Then, the total damage in time T is given by each attack a is

$\nu(a)^* d(a,\underline{\mathbf{s}})$;

where d = damage done per attack of type a given security measure **s** ignoring skill level.

The data needed to apply this model is a subset of the data needed for the earlier model that was developed and we shall discuss the data requirements and estimation issues below in a separate section. A number of assumptions and approximations will be needed before we can get the estimates we need even for this model, and one of the reasons that this model has been kept simple is to minimize the data requirements to estimate it so that it can be used.

The numerical estimation was carried out on a spreadsheet. Since no suitable data is available currently, the example uses hypothetical data for an organization. The data does reflect relative values in costs, damages and utilities that should hold in reality.

The cost data matrix {C} that was used is (in arbitrary monetary units)

---

[17] This assumes that all organizations have the same probability of being attacked. More generally we should sonsider the distribution of organizations by type, or $\omega(l) = N(l)/\Sigma_l N(l)$. It will also be useful to consider the distribution of cyber criminals by type, or $\alpha(a) = A(a)/\Sigma_a A(a)$. It may be that we can estimate the $\alpha(a)$'s more easily than the A(a)'s for each a.

C(r,q)	q=1	q=2
r=1	10	30
r=2	25	70

The degree of damage done {d}, in the same monetary units as the costs above, is given by the matrix

(a,k)	s (r,q)			
	1,1	**2,1**	**1,2**	**2,2**
1,1	20	60	10	30
2,1	15	40	8	25
1,2	40	120	20	60
2,2	30	80	16	50

In both the tables above, C and d are taken to be in monetary units (amortized) per unit time period. In the case of d this also implies that the victimization rate has been taken into account and the cells represent the product of the damage per attack and the rate of attacks experienced, by attack type, a.

The Utilities {U} to a malicious hacker are assumed to be given by

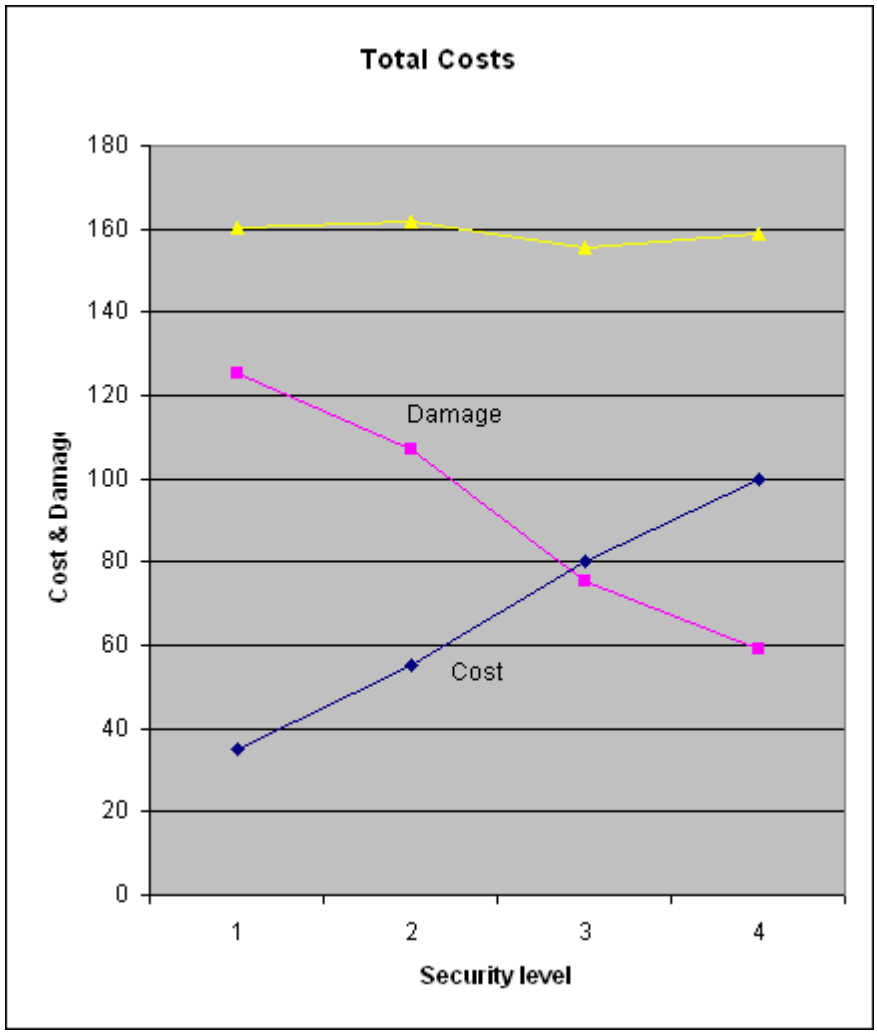
U(a,r,q)		q=1	q=2
a=1	**r=1**	.2	.1
a=1	**r=2**	1	.5
a=2	**r=1**	.5	.4
a=2	**r=2**	.3	.6

Results:

The model was run with the organization choosing different levels of security. We were interested to find the optimal level and type of security for the organization. Thus we varied the security posture (level and type) and computed the cor-

responding costs and damages. The point where the sum of costs and damages are minimized is of course the optimal posture. In this example, we find that a security posture of low level security for computing/communications and high level security for data is optimal. If the security level is increased beyond this level, the costs outweigh the expected benefits and the security is no longer optimal. This is illustrated in Figure 1 below

Figure 1. Total Costs versus Security Level showing Optimal Point



Managerial Insights

These results are of course specific for this model, its assumptions and the data used in the example. More generally, we can say that organizational policy can be

optimized through the use of such models. What we have observed is that increasing security levels excessively is not cost-beneficial. In other words, although damage could be reduced by enhancing security, after a point, the value of the marginal damage averted is less than the cost of the incremental security. Thus it is important for organizations to be able to estimate the marginal value of damages averted as they increase security. The marginal net benefit at some point will be less than the incremental cost of security, and the organization should not increase its security beyond this point. Of course, we have not taken risk averseness into account. However, for any finite risk-aversion, this result for optimality will hold. The optimal point may be shifted towards greater security. It is expected that risk-neutrality or risk-aversion will depend both on the sector to which the organization belongs and the organization.

Data Requirements for Analysis and Model Estimation

The more detailed model developed initially is too detailed and complex for estimation with current state of knowledge. However, it is important to develop such a model first as it indicates the data that we need to solve the problem of managing security. If we did not have the model we would not be aware of what our data requirements should be and unless we know of our requirements, we cannot design appropriate survey instruments. Keeping these more exacting requirements in mind, it is possible that future surveys can be developed and fielded so that the gaps in our knowledge are gradually closed.

We will need to apply aggregated models until the time when disaggregated data are available and we have already indicated some possible simplifications by dropping some indices. Even the simple numerical example highlighted the lack of basic data on cybercrime.

The data needed fall into two areas: the organization-related and the cybercrime process-related data.

A) Organization-related:

The data related to the organization {C, **s**, d} will either be known to the organization or will have to be collected by it. In principle, they can be obtained and indeed should be known by the organization in its own interest. C(**s**) (or C(r,q) or C(s)) is the cost of installing security measures to protect resource r at level q. This should be known to the organization from its systems managers and security systems vendors. Since s is derived from **s** as an ordered scalar variable, the incremental increase in C as s is enhanced [δ**C**/δs] should also be known.

s(r,q) is the actual security system installed by the organization, often called its security posture. The elements of the matrix **s** are (r,q) and indicate which level of security (q) the organization has chosen for each resource r. This again is obviously known to the organization at any point in time. This is the key decision variable for the organization, and its objective is to find the optimal value.

d(a,k,r,q) is the matrix that gives the extent of damage that could occur if an attacker of type a and skill level k commits a cybercrime of type a against an organization and if the organization had installed a security system of level q for resource r. In practice the most an organization can know is d(s|i) where i is the crime type that has been perpetrated. The matrix has to be complete and known, and the actual damage that would occur is read off from this matrix for a particular attack given a particular posture. The total damage in theory is D is $\Sigma_{a,k,r,q}$ d(a,k,r,q), remembering that q is an indicator variable. Again in practice the organization can only estimate D = Σ_i d(s|i). As already discussed, one method of estimating this is to anticipate what would be the impact of a given type of attack (the degraded state j), and what degree of damage would be suffered by the various resources (indexed by r) in state j. The organization must develop a methodology to estimate monetary values for these damages with reasonable accuracy and then estimate the expected damage under each type of attack. The organization may also wish to consider the set {e(i)} where e(i) is the systems entity targeted by crime type i. The mode of operation (MO) for a particular crime is also a significant factor and may be indexed by {θ}.

With proper detection and monitoring systems in place, an organization should be able to track the number of network intrusions and attacks it is experiencing per unit time, which is ν(l,s,i) where l is the type of organization, s is its security level and i is the crime type, as before. It is also important is to know δν/δs, the change in the attack rates as security is varied. Of course, an organization might experiment with different levels, or it may consult reports on network breaches and see in aggregate how organizations with different levels of security have fared in terms of attack rates.

B) Cybercrime process-related:

The parameters related to the cyber criminals are much more difficult to obtain. The number of attackers by type will vary over time, and it is only the active set that is relevant and that is what we imply by A(a,k). If we drop the index k, A(a) is the number of cyber criminals of type a. Again it would appear that this is difficult to estimate. However, a number of approaches have been developed in traditional criminology to try to estimate such numbers (active offenders) and such methods

may be applied to cybercrime in the future. One such approach is described with examples in Moitra 2005a and Moitra 2005b.

A further variable of interest is $\delta A/\delta s$, the change in the number of active offenders that might consider the organization as a potential target as the security level is changed. However, considerable care needs to be exercised to interpret this even in theory, since A is assumed to be the pool of all offenders (in a certain category perhaps), and not specifically those who would target a particular organization. We recall that the previously A was not taken as a function of s. On the other hand, there has been a suggestion in the literature that as the average level of security deployed by organizations rises, more and more potential cyber criminals will drop out because of frustration over the increased difficulty in committing cybercrimes, or their inability to commit the crime they intended. This dynamic aspect of A makes its estimation even more complex yet it is very important to take this into consideration.

U(a,k,l,s,i) or U(a,k,l,r,q,i) is the utility that a cyber criminal of type a with skill level k derives from committing a crime of type i against an organization of type l with a posture given by r and q (that is, s). While it is reasonable that this utility in theory will depend on a, k, l, r, q and i, it may be quite difficult (if not impossible) to estimate this function in practice. We shall discuss the estimation issues below. It may also be true that this utility depends on other factors. Knowing U, we can derive p, by assuming the logit model, or some other choice model, and hence λ. We also need to know $\delta U/\delta s$ and this may be even more difficult. This would represent the deterrence effect of network security. One can also calculate a possible displacement effect if some organizations increase their security levels relative to others.

Methodologies for Parameter Estimation from Available Data

We propose some approaches to the estimation problems that may be followed up in future research. The estimation of organization-related parameters has been discussed already. We would like to emphasize that it is extremely important for organizations to know their correct victimization rates. Firstly this is obviously important for their own security management. Secondly this is the basis of many reports on cybercrime. The rates reported by sampled organizations in the few surveys done so far appear to have many biases and the surveys themselves have many shortcomings (Koellisch and Jaehnke 2005, Moitra 2003). Good detection rates are to some extent a function of the security technologies used and the way security is handled at that organization (its policies and practices). The estimation of the sensitivity of victimization to installed security levels can be done at an aggregate level by observing the different attack rates against otherwise similar organizations that happen to have dif-

ferent levels of security. Alternatively, a survey undertaken to specifically to estimate this would offer a better solution to this problem. Finally organizations can observe the changes in attack rates against them as they change their security levels or even deliberately experiment with alternative security levels to estimate the effects. However, the data must be carefully collected, the correct statistical models must be used and the estimation process must be carried out carefully so that the true effects are measured.

The estimation of the cybercrime process-related parameters pose much greater difficulties, since it will be extremely difficult to survey cyber criminals and even if a sample of them are surveyed, their responses may be particularly unreliable. However, there are now many qualitative studies of hackers, malicious or otherwise, and some assessment of their characteristics may be gleaned from them (Biggs 2004, Douglas 2002, Hunter 2002, Power 2000, Smith, Grabisky and Urbas 2004). There are also some surveys and reports on cybercrime incidence, and some of the data reported in these may be utilized to develop estimates of the number of cyber offenders A and their individual offending rates λ (ignoring the indices).

One of the most problematic issues is estimating the number of active cyber offenders by type and skill level, A(a,k). Some attempts have been made to do this (Wall 2003, Moitra 2003) but further research is needed to arrive at better estimates. Alternatively, we might be able to get an estimate of the total number of active cyber offenders or perhaps A(a) from $\alpha(a)$ and $\Sigma_a A(a)$. Then we shall need to use additional data and assumptions to arrive at disaggregate estimates by offender type and skill level.

The sensitivity of the number of offenders to changes in security levels ($\delta A/\delta s$) will also be difficult to estimate. But this is a very important quantity for policy purposes. The optimal security policy of an organization depends very strongly on this. This actually represents two effects. One is the change in the number of offenders who will consider a particular organization (a kind of special deterrence) and the other is the change in the total number of offenders as the average security on the internet changes (something that we may term as general deterrence). That is, we should expect a drop-out effect as overall security on the Internet increases. It has been suggested that this has in fact been happening because the previously expected increase in network intrusions has not materialized.

According to rational economic and decision theory, an individual makes choices so as to maximize his or her utility, U. While there are many problems and difficulties with such a sweeping proposition, there is a large body of theoretical and empirical literature in economics, psychology, decision analysis and also criminology that suggests that behaviour can indeed be modeled according to such propositions of rational-

ity (Becker, Tommasi and Ierulli 1995, Hellman and Alper 2006, Lersch 2004). That is, with the exception of violent crimes, criminals do consider costs, benefits and risks in deciding whether to commit a crime. Independently, the qualitative literature on "hackers" suggests the same about their behaviour. This appears even more plausible since cyber offences almost always require preparation and hence premeditation. This utility function may vary significantly across cyber offenders, and therefore we need to estimate this function for each type of offender. In the model development above, we have suggested three generic types in terms of their sensitivity to security. A reasonably general model would be U(a,k,l,s|i), that is, the utility may be assumed to be a function of crime type, offender type, skill level of the offender, victim organization type and its security level. That the utility should be a function of the type of offender is axiomatically true. Whether the utility depends on the skill level may be debatable. However it is certainly plausible since a more skilled criminal may find it easier and possibly quicker to commit an offence. Further, the same category of offender (same a and k) may derive different utilities from attacking different types of organizations.[18] Similarly, the security posture of an organization may affect an offender's utility. Finally, again almost by definition, different crime types will provide different utilities. However, it has to be admitted that such a complex function may never be estimable at such a disaggregated level. The best we can do is to devise ways of approximating it on the basis of whatever relevant information we can obtain. Several approaches to measure individual utilities have been developed in econometrics and decision analysis and some of these methods may be applied.

Another key variable, or parameter of the model is p(a,k,l,s|i) – the probability of an offender in category (a,k) choosing a target that can be characterized by (l,s) for committing crime type i. In practical terms this is the function we are most interested in, since if we can estimate these probabilities, we can largely estimate the model. This is also the critically important quantity for the understanding of the cybercrime process. A combination of data on offender behaviour and observed network crimes may provide some indication of the nature of this function. If we can estimate p, we can then estimate λ, [generally $\lambda(a,k,l,s|i)$ or $\lambda(a,k|i)$] the individual crime commission rate based on some additional data and assumptions. Alternatively, we might be able to estimate λ directly from self-reports obtained from cyber offenders, in much the same way as has been done in traditional criminology (Burton, et al. 1999, Dunford and Elliott 1984, Jamieson, McIvor and Murray 1999, Menard and Elliot 1990). In all cases, there will inevitably be biases in the estimates as in almost all criminological data, and a

[18] For example, a hacker intent on committing financial fraud may derive very little utility from hacking the web site of an animal rights group, whereas an avid hunter may be more interested in breaking in into that web site.

further step would be to address these biases and compensate for them to the extent possible. Knowing any one of these quantities {U or p or λ} will allow us to estimate any other since they are related as shown above.

Estimating A, U (and/or p and/or λ) along with their sensitivities to security levels is very important for developing cyber policy in any case. For public policy and the control of cyber crime the sensitivities of these variables to legal sanctions (punishments, fear of detection/prosecution, etc.) is particularly important. We note that the total prevalence of cybercrime over any unit time period is represented by $\Lambda = \lambda * A$.[19]

We emphasize that the model is not very complicated but the data required to estimate it is a major hurdle at this point in time because of the paucity of cybercrime data. Simpler and more approximate models may be estimated, as we have discussed, from the little quantitative data we do have and the qualitative data that can be examined. Thus we have a number of estimation problems where we face the general challenge of estimating parameter values from qualitative findings. Almost certainly, we shall have better data in the future, and a model such as the one we have developed may be estimated, perhaps with some modifications. That would then lead to organizations being able to make better decisions regarding their network security.Future research needs to focus on these problems of estimating these key quantities from available data. The greater the degree of disaggregation in the data, the better the analysis that we can do. There should also be a policy of making collected data available to researchers. Policymakers should urge organizations and agencies to make available their data (usually collected from public funding, directly or indirectly).

Summary and Conclusions

Summary

In this paper we have identified and discussed two distinct kinds of responses to cybercrime. One is the public response through the development of cyber laws and policies on Internet governance. The second is the response of organizations taking decisions to safeguard their assets that are vulnerable to network crimes. We have referred to this as the private response even though public organizations are involved because they are acting on their own and are not involved in law-making that would apply to all parties in their jurisdiction.

[19] Also, if we take s as the level of sanctions, then the above model can be used for developing optimal sanction levels.

The concerns of public cyber policy are to enforce law and maintain order with respect to the Internet (or cyber space) for the general good of society. Two particular goals are to ensure that all members of society benefit from the Internet and that e-commerce can reach its full potential. The concerns of organizations are to control network attacks and crimes against them and to reduce the damages caused by such actions. In order to develop the most appropriate policies or to make the best security decisions, both policy makers and organizations have a common need for reliable and detailed data on the prevalence and patterns of cybercrime. This paper discusses this data and how it might be obtained in some detail.

The focus here has been on security management for organizations. We have introduced the notion of an optimal level of network security for a given organization. The issue of finding an optimal security system is extremely important for organizations since many may gravitate to unnecessarily costly security systems due to excessive fear. This fear may be generated by the media publicity given to cybercrime and may be fed by vendors selling network security systems to organizations. The model presented here would allow for a more objective decision.

The paper has developed an integrated modeling approach for exploring this optimal level for an organization. To the best of our knowledge, this is the first time such a model (or any model like this) has been developed for cybercrime. The model has taken a comprehensive set of factors into account. Thus it considers the prevalence of different types of cyber criminals, their individual crime rates, their choice process in targeting victims, and it also postulates a function to represent the utility they may derive from committing cybercrimes. The model also considers various factors associated with security management from the perspective of organizations such as the victimization rate, the damage caused by network attacks and the costs of alternative security measures. This approach will enable organizations to find the most appropriate level of network security. In essence, we apply policy analysis techniques and optimization methods to help organizations analyse security decisions.

An illustrative example was presented to show this approach can work in practice for organizations. This can be used as an initial template by organizations and can be adapted to suit individual situations. The example shows that under reasonable assumptions there is indeed an optimal point where the total costs to an organization is minimized. In other words, after some point the incremental benefits of greater security becomes less than the incremental costs. This concept of an appropriate level of security is important for organizations in managing their network security efficiently. The solution procedure to find the optimal point has been discussed in the appendix.

The data needed to estimate the model have been identified. This has highlighted the information on cybercrime that is important to obtain for a better understanding of the

phenomenon, whether for organizational decisions or for policy making. In addition, we have identified the data needed by organizations to make appropriate security decisions such as the expected damage resulting from a cyber attack and the cost of security measures. A key set of parameters required for effective policy or decisions are related to the sensitivities of cyber criminal behaviour to policy or decision variables. Finally the analysis of the data requirements shows the connection between organizational security management (which is essentially private) and public cyber policy that includes cybercrime control, cyber law enforcement and Internet governance.

The paper has suggested methodologies for obtaining the data that is needed. Someorganization-related data are relatively easy to obtain while some of these may be more difficult. However, it is clear that the data related to the generation of cybercrime that are also needed for policy-making will be extremely difficult to obtain and assess. However, in analogy with traditional criminology, some directions for collecting such data have been discussed.

Conclusions

One of the main conclusions of this study is that it is quite possible that security is being "oversold" to many organizations. In general there should be an optimal point such that it is not cost-beneficial for an organization to spend more money on security. The marginal returns on greater expenditures on security will tend to decrease as is the case for most systems and this implies the existence of an optimal point under reasonable assumptions. It may well be that this pint is achieved at relatively modest levels of security for many organizations, but unless this kind of analysis is done, this optimal point will not be discovered. In other words, the philosophy of "more is better" is not necessarily true. While there can be pressures on organizations from various sources such as security systems vendors or even its own systems managers, organizations need to decide independently what is best for them through rigorous and objective analysis.

The second conclusion we can draw is that we need better cybercrime data for effective and cost-beneficial decisions whether for public cyber policy or for private security management. As the illustrative example showed, the current data is quite inadequate to estimate even a very simple model. This exercise has identified specific variables and parameters that should be estimated for effective decisions. The magnitude of the sensitivities of offender behaviour parameters to policy and security decisions is an open issue. We do not have any idea of their values and it is extremely important that we attempt to estimate these sensitivities. The analysis reported here can be used for designing better cybercrime surveys to do this in the future.

The third conclusion and one of the contributions of this paper to the cybercrime literature is that organizational security decisions are an important aspect of controlling cybercrime and its impact. We have highlighted this by showing that both the prevalence of cyber offenders and their rate of offending should be expected to depend on the security measures organizations adopt. That is, not only will the victimization rate and the expected damages from cybercrimes be reduced through security, but the cyber criminal activity overall should be reduced as the aggregate level of security on the Internet increases.

Finally, in terms of future research, we have already noted that the model proposed here should be developed further. Surveys and collection methodologies have to be designed to collect the necessary data, and more research is needed to analyse the solutions we obtain from the model as these solutions represent recommended decisions for managing network security for organizations.

References

ANANDARAJAN, M., TEO, T.S.H. AND SIMMERS, C.A. (Eds.) 2006. *The Internet and Workplace Transformation*. M. E. Sharpe, London.

AUSCERT. 2007. *The 2005 Australian Computer Crime and Security Survey*.

BARFIED, C.E., HEIDUK, G. AND WELFENS, P.J.J. 2003. Internet, Economic Growth and Globalization. Springer Verlag.

BAZARAA. M. S., SHERALI, H. D. AND SHETTY, C. M. 2006. *Nonlinear Programming: Theory and Algorithms*. Wiley Interscience, New Jersey.

BECKER, G., TOMMASI, M.AND IERULLI, K. 1995. *The New Economics of Human Behaviour* Cambridge University Press, Cambridge.

BERNASCO, W. AND NIEUWBEERTA, P. 2005. How do residential burglars select target areas? British Journal of Criminology, Vol. 44, 296-315.

BIGGS, J. 2004. *Black Hat: Misfits, criminals, and scammers in the Internet age*. Apress, Berkeley.

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.

BRENNER, S.W. AND SCHWERHA, J.J. 2004. Introduction – Cybercrime: A Note on International Issues. *Information Systems Frontiers* 6:2, 111-114.

BROADHURST, R. 2006. Developments in the global law enforcement of cybercrime. Policing: An International Journal of Police Strategies & Management, Vol 29 (3) 408-433.

BROADHURST, R. AND GRABOSKY, P. 2005. *CYBER-CRIME: The Challenge in Asia*. Hong Kong University Press, Hong Kong.

BURTON, V. S. JR., EVANS, T. D., FRANCIS T. CULLEN, F. T., KATHLEEN M. OLIVARES, K. M. AND DUNAWAY, R. G. 1999. Age, self-control, and adults' offending behaviors A research note assessing *A general theory of crime.* Journal of Criminal Justice , Vol., 27, 1, Pages 45-54.

CANGEMI, D. 2004. Procedural law provisions of the Council of Europe convention on cybercrime. International Review of Law, Computers & Technology, Vol. 18, No. 2, pp 165-171.

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

CSI 2007. *The 2007 CSI Computer Crime and Security Survey*.

DEVEZAS, T.C., LINSTONE, H.A. AND SANTOS, H.J.S. 2005. The growth dynamics of the Internet and the long wave theory. Technological Forecasting and Social Change, Vol. 72, No. 8, pp 913-935.

DOUGLAS, T. 2002. *Hacker Culture*. University of Minnesota Press, Minniapolis.

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

DUNFORD, F. W. AND ELLIOTT, D. S. 1984. Identifying career offenders using self-reported data. Journal of Research in Crime and Delinquency, 21, 57-86.

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;

HELLMAN, D. A. AND ALPER, N. O. 2006. *Economics of Crime: Theory and Practice*. Pearson Custom Publishing, Boston.

HUNTER, R. 2002. *World Without Secrets*. Wiley, N.Y.

JAMIESON, J., MCIVOR, G. AND MURRAY, C. 1999. Understanding Offending Among Young People. Social Work Research Findings No. 37. Scottish Executive Central Research Unit, Edinburgh.

JUNE, W. 2005. Internet penetration analysis: the impact of global e-commerce. Global Competitiveness, Vol. 13, pp 9-24.

KOELISCH, T. AND JAEHNKE, J. 2006. Cybercrime gegen Organisationen: Ergebnisse auslaendischer Viktimisierungsuntersuchungen and Ueberlegungen fuer einen Survey in Deutschland. Monatsschrift fuer Kriminologie und Strafrechtsreform, Vol. 89, No. 5, pp 366-388.

KOOPS, B-J. AND BRENNER, S.W. (Eds.) 2006. *Cybercrime and Jurisdiction: A Global Survey*. T.M.C Asser, The Hague.

LERSCH, K. M. 2004. *Space, Time and Crime*. Carolina Academic Press.

LESSIG, L. 2000. *Code and Other Laws of Cyberspace*. Basic Books, New York.

LOOMIS, D.G. AND TAYLOR, L. D. 2001. *Forecasting the Internet: Understanding the Explosive Growth of Data Communications*. Springer Verlag, Heidelberg.

LUENBERGER, D. G. AND YE, Y. 2008. *Linear and Nonlinear Programming*. Springer Publishing, New York.

MACGREGOR, R. AND VRAZALIC, L. 2007. E-Commerce in Regional Small to Medium Enterprises. IGI Publishing, Hershey, PA.

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

MENARD, S. AND ELLIOT, D. S. 1990. Self-reported offending, maturational reform, and the Easterlin hypothesis. Journal of Quantitative Criminology, Vol. 6, No. 3, 237-267.

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. 2004. Internet Crime: Towards an Assessment of its Nature and Impact. International Journal of Comparative and Applied Criminal Justice, Vol. 28, No. 2, pp 105-123.

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.

MOITRA, S. D. 2007. An Optimal Network Security Management Model for E-Commerce. INFORMS, Seattle, 2007

http://www.iimcal.ac.in/res/upd/WPS%20615.pdf

MOITRA, S. D. AND KONDA S. L. 2004. An Empirical Investigation of Network Attacks on Computer Systems. Computers & Security, Vol. 23, pp 43-51.

NEWMAN, G. R. AND CLARKE, R.V. 2003. *Superhighway Robbery: Preventing E-commerce Crime*. Willan, Cullompton.

PATTAVINA, A. 2004. *Information Technology and the Criminal Justice System*, Sage Publications, Thousand Oaks, CA.

POWER, R. 2000. *Tangled Web: Tales of digital crime from the shadows of cyberspace*. Que Corporation, Indianapolis.

PRICE, M.E. AND VERLUST, S.G. 2005. *Self-Regulation and the Internet*, Kluwer Law International, The Hague.

SAMORISKI, J. 2002. *Issues in Cyberspace: Communication, technology, law & society on the Internet frontier*. Allyn & Bacon, Boston.

SCHELL, B.H. AND MARTIN, C. 2004. *Cybercrime: A Reference Handbook*. ABC – Clio, Santa Barbara, CA.

SMITH, R.G., GRABOSKY, P. AND URBAS, G. 2004. *Cyber Criminals on Trial*. Cambridge University Press, Cambridge, UK.

SOMMER, P. 4. The future for the policing of cybercrime, Computer Fraud & Security, Vol. 2004, (1) 8-12.

SPINELLO, R. A. 2002. *Regulating Cyberspace: The Policing and Technologies of Control*. Quorum Books, Westport, CT.

SURI, R.K. AND CHHABRA, T.N. 2003. *Cyber Crime*. Pentagon Press, New Delhi.

TAYLOR, R.W., CAETI, T.J., LOPER, D.K., FRITSCH, E.J. AND LIEDERBACH, J. 2006. *Digital Crime and Digital Terrorism*. Pearson/Prentice Hall, Upper Saddle River, N.J.

THOMAS, D. AND LOADER, B. D. 2000. *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge, London.

TRAIN K 1986. *Qualitative Choice Analysis: Theory, Econometrics and an Application to Automobile Demand*. MIT Press, Cambridge, MA.

United Nations 2002. General Assembly Resolution 56/121: Combating the criminal misuse of information technologies. New York.

United Nations 2003. General Assembly Resolution 57/239: Creation of a global culture of cybersecurity. New York.

UNCTAD 2005. Information Economy Report. Geneva.

WALDEN, I. 2004. Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law and Criminal Justice, Vol. 12/4, pp 321-336.

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.

WALL, D. S. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, Cambridge, UK

WESTBY, J. C. 2003. *International Guide to Combating Cybercrime*. American Bar Association, Chicago.

YANG, D. W. AND HOFFSTADT, B. M. 2006. Countering the cybercrime threat. American Criminal Law Review, Vol. 43 (2) 200-215.

YOUNT, L. (Ed.) 2006. Does the Internet Increase the Risk of Crime? Thomson/Gale, Greenhaven Press, Farmington Hills, MI.

Appendix:

Deriving the solution to the problem of finding the optimal security level.

The objective is to **minimize Z = D + C** with respect to security level s (Moitra 2007).

The solution will be at the point where

$\delta \mathbf{Z}/\delta s = 0$ or when

$\delta \mathbf{D}/\delta s = -\delta \mathbf{C}/\delta s$

The left hand side, $\delta \mathbf{C}/\delta s$, is the change in costs as the security levels are changed and will have to be obtained from vendors or internal sources. In practice, C will not be a continuous variable and the changes will be discrete. However the (discrete) changes in costs should be known in theory. The right hand side may be written as

$\delta \mathbf{D}/\delta s = \delta(d*\upsilon)/\delta s$, since $\mathbf{D} = d*\upsilon$

where d is the expected damage per attack (written as d(i|s) above) and υ is the rate of attacks. Again, for simplicity of the derivation, we are dropping all the indices (a, k, l, and i) as explained earlier.

Expanding, we have $\delta \mathbf{D}/\delta s = (\delta d/\delta s)* \upsilon + (\delta \upsilon/\delta s)*d$

Now $\upsilon = p*A*T/N$ (the number of victimizations over time T per organization)

Therefore, $(\delta \upsilon/\delta s) = T/N\{(\delta p/\delta s)*A + (\delta A/\delta s)*p\}$

From our earlier expression for p in terms of U, we have

$\delta p/\delta s = (\delta p/\delta U)(\delta U/\delta s)$

And $\delta p/\delta U = \{expU/(1+expU)^2\}$

Finally, substituting in our basic condition for optimality, $\delta \mathbf{D}/\delta s = -\delta \mathbf{C}/\delta s$ (as above), we have

$(\delta d/\delta s)* \upsilon + d*(T/N)*[\{expU/(1+expU)^2\}*(\delta U/\delta s)*A] + (\delta A/\delta s)*p = -\delta \mathbf{C}/\delta s$

The solution is to set s such that the above holds. Since this is an implicit equation in s, it has to be solved numerically. Several suitable packages (to solve non-linear equations as this) are available and given the input data that is required, along with some trial and error with starting values, the equation can be solved reasonable easily.[20] In

[20] It is of course important to check whether a solution exists and that the functional properties required to solve this problem are satisfied. For details on nonlinear optimization, a stan-

practice the values of s and C will be discrete. An alternative method could be conducting an exhaustive search over all possible values of s (which may not be that many) as was done in the numerical example above. The important obstacle is to get the required input data. However, many of the data items can be estimated by an organization, and the others may be estimated from the available data on cybercrime with some approximations. In the paper we have discussed the particular data items needed. If the required data on cybercrime were available, as we have discussed, then the above optimization problem can be solved. The solution will of course always be subject to the assumptions made in the process of deriving this model and this solution. In the text of the paper, we have discussed and interpreted each of the terms in this last equation.

dard text on the subject may be consulted (Bazaraa, Sherali and Shetty 2006, Luenberger and Ye 2008).