INTERNET AND COMPUTER RELATED CRIME: ECONOMIC AND OTHER HARMs TO ORGANIZATIONAL ENTITIES

Edward M. Roche*

There are different and conflicting reports estimating the value of Internet fraud [and related computer crime]. But serious issues abound regarding calculation of values. Here, cost estimations are broken down into three categories: (1) tangible, (2) intangible, and (3) operational. For each of these categories, we sub-divide into different classes of harmful effects, and then suggest several ways of making estimates. These include such approaches as (a) adjustment of under-reporting data, (b) use of insurance values to estimate reputation loss, (c) time & effort estimations for individuals [and many others]. We suggest how these estimations might be used in victim compensation, defined as either (a) government victims, (b) institutional victims [including business enterprises], and (c) individual victims. A major theme that emerges from this analysis is that (1) some of the considerably larger damages [costs] are more difficult to estimate, since they are speculative in nature, and (2) damages [costs] that occur either (a) internally [e.g., for the individual, inside the enterprise], or (b)

* Information Policy Institute, Chapel Hill, North Carolina, Director of Scientific Intelligence, See http://www.infopolicy.org. Home address: 135 East 54th Street, Suite 4-B, New York, New York 10022-4509 Tel: 646-416-6592. We would like to thank Mark Halligan, Chairman of the ABA Committee on Trade Secrets for providing information regarding trade secret protection and calculation of damages.
more distant in time, from a practical point of view, generally in the absence of advance planning are extraordinarily difficult to calculate.

I. The Butterfly Effect

It simply is not possible to know the true cost of internet fraud [and related computer crime]. But it may be possible to estimate its value.¹

In an ideal scenario aimed at making this estimation, we first define the scale and scope of the types of crimes being discussed. Then, for each type of computer crime, we discuss the adequacy of known data, the sources of error in the reporting, the reasons for those errors, and what can be done to correct the estimates. We then make estimates for each type, and add them together.

Although an overall sector-based approach to the problem might prove to be overly general, it represents a way that promises to yield a useful approximation of costs and value lost that is more accurate than the general overall summary figures reported in the press. It is a taking apart of those numbers.

Before going further, however, let's explore data from a series of interviews. Four examples are presented below. They will clarify how the costs involved range in nature from highly specific to highly speculative.

A. Example One: Reputational Loss

Let's start with an example of a U.K. bank that suffered an Internet fraud. It is a true case, but the name of the bank

¹ The Butterfly Effect is a phrase that encapsulates the more technical notion of sensitive dependence on initial conditions in chaos theory. Small variations of the initial condition of a dynamical system may produce large variations in the long-term behavior of the system. This is sometimes presented as esoteric behavior, but can be exhibited by very simple systems: for example, a ball placed at the crest of a hill might roll into any of several valleys depending on slight differences in initial position. Wikipedia.com, Butterfly Effect, http://en.wikipedia.org/wiki/Butterfly_effect (last visited Oct. 31, 2006).
A major European bank suffered a compromise of its computer system when hackers managed to break in and deface one of the internal web sites. There was no direct economic loss to the bank. However, in line with regulatory and insurance requirements, the bank reported the incident. When word got out to “the street,” e.g., to the financial markets, there arose a perception that the bank was unable to secure its information systems, and thus might pose a risk to investors. Consequently, the share price of the bank started to fall.

Unfortunately, at this time, the bank was the subject of a hostile takeover bid from a rival bank. The predator was able to take advantage of this drop in share price and make a successful move in the market, thus acquiring the bank. Even though no money was lost due to the computer hack, the bank was sold off and lost its autonomy in the marketplace. The bulk of its top management was made redundant.

The question that begs asking is this: If no money was taken from the bank, then how can there be a claim for financial loss? The hackers never were caught, so the issue did not arise. But there is the issue of possible insurance coverage.

To make matters even worse, subsequent auditing revealed that the entire incident might not have happened as first reported. Unfortunately, this “subsequent auditing” was done after the takeover was completed!

Clearly there was “loss,” but it was a secondary effect of the reputational loss which itself was caused by the hint [later determined to be false] of a security weakness in the bank’s system.

This example points to several issues including:

1. If there was no financial loss, e.g., no money stolen, then can the reputational effect be consid-
2. If it is considered, then what is the basis of the loss calculation? For example, should it be the lessening of the value of the company in the stock market [or effects even beyond that]?

3. If the bank eventually was taken over, then were there additional damages that might be considered?

4. Are damages to the shareholders or to the bank itself, or to yet others?

5. Finally, if it could reasonably be expected that leakage of the facts to the financial markets might harm the share value of the company [in such a catastrophic way], then is it a responsible action to report, or is it more prudent to hold back the information?

B. Example Two: Failure to Report

The Chief Information Officer of a large and well-established Swiss bank discussed his focus on computer security and the requests by some governments concerned about illegal money-laundering that their investigative services be given access to those encryption codes used for money transfers:

If our customers ever learned we were cooperating with governments in this manner, we would lose all credibility in the marketplace. Customers come to our bank with a firm belief in the absolute security and confidentiality of their transactions. If anything at all changed this perception, it would be a disaster for us, and it would take an indefinite amount of time to recover.

---

2 Calkins lists reputation effect as one of the elements of an economic analysis of hacking. See Mary M. Calkins, They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models, 89 Geo. L.J. 171 (2000).

3 The Chief Information Officer (CIO) in most companies is responsible for the acquisition, management, and operations of all data processing and telecommunications throughout the enterprise. For [large] multinational corporations, the CIO might have several hundred persons reporting to them, and an annual budget of several dozen million dollars.
Even in these "private" and "off the record" discussions, the interviewee never made an admission of a security problem. But when asked about the situation in the industry, the CIO emphasized that it is never in the interest of a financial institution to report security problems. He believes the best way to cope with this situation is through "internal" processes.\(^4\)

This example raises several questions including:

1. If the majority of organizations resist reporting Internet fraud [and related computer crime], then what is the meaning of reported crime statistics? For example, should any number reported be assumed to represent only a fraction of the actual problem? [Most would say "yes."]

2. Is it possible that the long-term damage from a relatively minor information security compromise might be far greater than the immediate harm that is inflicted? If so, then what can we conclude from a comprehensive report on the levels of immediate harm reported? Are we [again] only making an examination of a fraction of the actual amount?

3. What is the best strategy: to never report, or to invest much more in security in hopes that pre-

vention can work and avoid any embarrassment.

C. Example Three: Asymmetric Defense Costs

The manager of an important IT installation\(^5\) was discussing the rapid increase in costs associated with defending against Internet fraud. He pointed out first the problem that it is impossible to have complete security, no matter what precautions are taken.

*No matter how much we spend, we can never have complete security. All spending can do is LOWER THE PROBABILITY of a successful computer attack, but it can NEVER stop completely the problem. Eventually, any organization will reach diminishing returns on their security investments. We end up spending too much and getting in return virtually no increase in security.*

Second, he lamented the dilemma of so-called “asymmetric defense” issue:

*Our problem is that it costs so little to launch an attack, and so much to defend against it. It is much like the failed attempts at strategic missile defense—a losing proposition. We can NEVER obtain complete security, even if we had unlimited resources, which we don't. THE ONLY QUESTION IS HOW MUCH INTERNET FRAUD CAN WE TOLERATE. THIS IS FOR MOST A VERY DIFFICULT QUESTION TO ANSWER, PARTICULARLY IN THE BOARDROOM.*

This example raises several questions including:\(^6\)

1. Is it possible for an organization to define the level of Internet fraud [and the damage] it is willing to tolerate?
2. Who is empowered to make the decision regarding

\(^5\) IT—“Information Technology”—a term used to represent all of the computing and telecommunications resources within an organization.

the level of security required, and the level of vulnerability allowed?
3. Should the cost of Internet fraud include the costs of defensive measures, even if no fraud takes place because the defenses appear to be effective?
4. And if defensive measures are included in the cost estimations, then how far does the analysis reach? For example, within the IT function alone? Throughout the enterprise? Hardware and software costs? Training and awareness costs? All security measures?

D. Example Four: Compromise of Individual’s Information

In a large North East US based insurance company, several of the top executives started to get strange credit reports and bank notices. Evidently many had taken out mortgages, topped out their credit cards, and purchased many fancy consumer goods they had no recollection of ever needing.

Later investigation revealed that a trusted employee was the source of the information used to compromise the identity of hundreds of employees. As a database administrator [who had access to all personal information on the company employees], the employee sat in a cybernetic “cats bird nest.” The information had been “brokered” to organized crime, then used in a variety of scams. The organizational leadership was shocked.

“How could one of our most trusted employees do this? and Why?”

Any security consultant easily could have given them the answer. All of the “usual” reasons applied:

1. Gambling debts that must be paid off to the mob.
2. Resentment at not getting a promotion.
3. Anger at the company for not paying enough money “while top executives get rich.”
4. Psychopathic behavior.
In this case, the “resentment” answer proved to be the best fit. For the company, firing the director of security was only the first step in a very long chain of events—investigative costs, litigation, administrative costs to improve security, re-screening of “trusted” employees, calling in a security consulting firm to “fix” the problem, conducting numerous “audits” to see if other problems could be detected, paying money to “public relations” consultants to make sure the reputational effects were minimized, e.g., “this was a freak accident, an aberration in behavior of a single employee, and not representative of our overall security”—all of which added up to a large number that never was completely calculated, and certainly never made public.

What was the “cost” of the attack: zero.

What was the “effect” of the attack: millions.

This example also raises questions regarding the cost of this Internet fraud crime. These include:

1. What is the total financial cost of this crime; what should be included and excluded?
2. How many crimes were there in all? [e.g., what is reported in the crime statistics?]
   (a) Initial theft of corporate information?
   (b) Conversion of the stolen information?
   (c) Use [by others] of the information for fraudulent purposes?
   (d) Individual crimes committed “downstream” from the original theft?
3. Should all of the investigative costs get included?
4. Should all legal and administrative costs be included?
5. In general, how wide should the circle of secondary effects be traced in order to evaluate the cost of this Internet fraud case?
6. When the database administrator is prosecuted, then how wide is drawn the circle of responsibility?
II. Classes of Loss

These examples and many others suggest several ways to characterize the losses from Internet fraud and abuse. In particular, they might suggest at least three major categories of loss. (See Figure 1 below.) These are:

Tangible Losses. When Internet fraud is used to steal property, particularly to take delivery of illicitly gained goods, there is a tangible and identifiable type of loss. Although more abstract, the theft of services may fit in this category (and is easy to measure).

Intangible Losses. Internet fraud can cause serious damage without the theft of any property. In some sectors, such as banking, the reputational effects might be the largest to contend with. What is the complete range of intangible loss?

Figure 1: Categories of Losses from Internet Fraud
OPERATIONAL LOSSES. Any discovered loss\(^7\) of necessity requires the expenditure of at least a minimum amount of resources in order to get back to normal. In addition, there is a significant amount of cost for general administration of security, including during the “clean up” phase after discovery of a compromise. What might be the details of this and what value does it comprise?

A. Tangible Losses

Internet fraud in many cases is aimed at the illicit taking of goods or services. Note that this objective is very different from computer crimes that deny services to others. The most popular of this class of loss is the stealing of money, every hacker’s dream. According to a banking source:

One of the first great computer crimes involved a programmer who re-wrote the interest calculation in a bank’s savings accounts to take the $1/1000-ths of a percent remaining from each interest calculation and have it transferred to a secret personal account. For a while they made lots of money, but it was difficult to say if they stole money, or simply created money from adding up multiple small transactions.\(^8\)

This type of crime still is with us today, with a similar theft taking place recently against a New York bank orchestrated by a gang of Russian hackers.\(^9\) In another case, a programmer changed the shipping information for delivery of telecommunications equipment to a “dummy” warehouse. Millions of dollars of equipment was delivered [and subsequently diverted] before discovery of the crime.

We can say that depending on the type of fraud, real tangible losses may account for a considerable amount of loss.

---

\(^7\) Note that it is estimated than less than 10% of Internet frauds are detected.

\(^8\) Unfortunately, this rather fine legal distinction did not sit too well with the police and prosecutors who handled the case.

\(^9\) It always is quite interesting to read the published accounts of computer fraud, with particular attention paid to any public statements made by the victim financial institution.
In addition, depending on how it is defined, the theft of services can as well be significant, although with increasing levels of computer security in society, this option each day is lessening as a possibility.

For the most part however, the valuation of the losses can be estimated by simply taking into consideration either the book value of the items, or the service cost as a function of the amount of time used [or another relevant metric].

B. Intangible Losses

Perhaps it is fitting that for hostile activity as abstract in its nature as is Internet fraud [an almost completely “information crime”], the largest losses might be “intangible,” also of an “informational” nature. We can identify as among the most important two categories of intangible losses: (a) Reputational Losses; and, (b) Intellectual Property Losses.¹⁰

REPUTATION. In the second example—Failure to Report—we can see how the release of information regarding a relatively minor security incident can have disproportionate effects on an institution. There can be both long-term and medium-term effects. Examples would include:

1. Drop in the market capitalization of the firm as word “gets out” that has some type of security problem. Investors are unlikely to put their money back in until they are reassured, but for many, given the vast amount of investing possibilities, the problem even if fixed might deter re-investment.
2. Long-term “tarnished” effect on the firm where a reputation earned tends to “stick” in the minds of investors and customers, thus leading to permanent damages [in

¹⁰ See Michael L. Rustad & Thomas H. Koenig, Rebooting Cybertort Law, 80 WASH. L. REV. 335, 362 (2005) (“The injury problem in cyberspace is based on intangible losses, unlike the disfigurement or pain and suffering experienced by the victims of physical injury. Nevertheless, these economic or information-based injuries are legally protectable interests.”). For examples of specific loss calculations, see Reid Skibell, Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act, 18 BERKELEY TECH. L.J. 909, 932 (2003).
business (or other activities)].

**INTELLECTUAL PROPERTY.** Divided into three categories—(1) patents, (2) copyright, and (3) trade secrets—losses of intellectual property can have long-term and devastating effects on an enterprise. Generally there is a good understanding [and substantial historical record] for estimating the cost of patent and copyright violations.\(^{11}\) Regarding patents, for example, one executive interviewed said:

> We found that a Japanese company had copied completely our patented design, but they were so large, and we were so small, the prospects of litigation seemed daunting. Their production quickly out-paced ours, and then they started to modify and re-patent our ideas. When we went to the U.S. government for help, they turned a deaf ear. In balancing overall U.S. interests against our company’s interests, guess who came out on top? At the time, the relationship with Japan was too sensitive to “rock the boat” with a case like ours. Eventually, we lost everything.

However, in the case of trade secrets, a more complicated picture emerges. These “secrets” include [but are not limited to] the following types of information [and data]:

1. Customer lists;
2. Sales forecasts;
3. Workflow documentation;
4. Employee lists [and other details on employees (such as executive compensation)]; and,
5. Special knowledge for either manufacturing or other work processes.

Trade secrets consist of a very large range of types of data and information, and there is a corresponding great variety in the motives and uses for stealing them.\(^{12}\)

\(^{11}\) No need to discuss herein.

\(^{12}\) Types of persons interested in trade secrets include: competitors who want
Unfortunately, valuation of trade secrets is problematical. Two examples will illustrate the reasons:

*TIME VALUE.* Over time, information that is a trade secret might become more valuable [or decline in value]. The result is that any *declared* value of the trade secret will diverge from the recorded [or declared] value.

*EXTERNALITIES.* Your trade secrets may change in value [may become worthless] depending on events you do not control, such as activities of competitors. What is valuable one day may be worthless the next. [NB: Related to "time value."]

*SLOPPY ACCOUNTING.* It is a fact that most corporations have not valued their trade secrets. If this is the case, it is difficult under examination to sustain the idea they are trade secrets at all, since by definition in order to be a trade secret, it must have value *that can be documented.*

In any case, it is the loss of trade secrets, whether valued or not, that potentially leads to the most chilling long-term consequences for the victim.

*C. Operational Losses*

The two major types of operational losses that are incurred as a result of Internet fraud [and related computer crimes] involve the activities that are compelled [to take place] as a consequence of the incident and the changes in operations that must be put into place in order to insure against any repeat of the event.

We have classified these as: (a) administrative recovery expenses, and (b) security administration [expenses].

*ADMINISTRATIVE RECOVERY.* As a consequence of any event, there is an immediate *forced* requirement that the organization take all necessary measures to bring the situation back to nor-
mal. This would include activities such as:

1. Impounding of all internal records associated with the event.
2. Collection of statements from persons who have knowledge of the event.
3. Electronic data discovery and computer forensics.
4. Analysis of the electronic discovery.\textsuperscript{13}
5. Legal expenses such as (a) preparation of complaints, (b) all of the ‘downstream’ activity associated with litigation.
6. Filing [and sustaining] insurance claims associated with the event.
7. Mobilizing [if needed] the public relations capabilities of the firm, including potentially the “crisis management center” to deal with the public [including financial analysts].
8. As needed, coordination with law enforcement [or other government authorities].

For these types of expenses, it would be customary to have easily a clear accounting of any external resources [advisors, experts] used, but for internal resources of the firm, it is critical that a pre-arranged system be in place to account for the organization’s personnel involved and their time commitment.\textsuperscript{14}

\textit{Security Administration.} All organizations [even many individuals] have security expenses of one type or another. Should security fail, it signals that something has grossly failed, and consequently there is a need for a mandatory investigation, and revision of the procedures [or technologies] involved. In the case of Internet fraud [and related computer

\textsuperscript{13} This can be extraordinarily expensive, and usually is done by outside [highly paid] experts.

\textsuperscript{14} If this is not accounted for immediately upon initiation of the recovery operation then it is likely the real cost will never be credibly sustainable, e.g., there will be a complete absence of records to substantiate the claim.
crimes], this involves several “sub-systems” of the security apparatus including:

1. **ADMINISTRATIVE PROCEDURES.** The organization must assess whether or not any administrative procedures failed. Examples would include: (a) accidental disclosure of confidential information, (b) vulnerability to a “social engineering” attack,15 (c) failure in screening out criminal personnel, or to watch for signs of a compromised employee, (d) failure to train adequately personnel to protect information or systems, (e) human error in administering what is otherwise a relatively secure system.

2. **INFORMATION SYSTEMS.** Computer networks are protected by [among many other technologies] so-called “firewalls” that read through incoming data traffic to screen out malware or other types of threats. It is an unfortunate fact of life that firewalls [and other administrative software] can detect only known threats. Consequently, if a “hack”16 is used for the first time, then no installation can have protections against it, and the threat will not be recognized.

Firewalls receive in the press much recognition, but the largest expenditures in IT security include (a) password and access administration, including “help desk” services, (b) software and hardware systems that monitor and control network and system security, (c) the cost of designing, building and maintaining systems with excessive security [because the “hackers” leave one no alternative but to expend these costs.] NB: in many cases, item (c)

---

15 **SOCIAL ENGINEERING** is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible. Wikipedia.com, Social Engineering, http://en.wikipedia.org/Social_engineering_%28security%29 (last visited Oct. 28, 2006).

16 Literally, a way of cutting through or “hacking through” computer security.
is the greatest because it involves re-design of entire systems.

When an incident occurs involving information systems, it usually calls for costly replacement or upgrading of equipment and systems. For most companies, this type of expenditure is a "must do" spend, and in many sectors [e.g., financial services] it is a required project [in order to maintain compliance with Federal regulations].

After an incident occurs, the organization must engage in a "mopping up" operation in which the information system—in a large enterprise comprised of thousands of computing devices is "sanitized" of any offending malware [or otherwise made invulnerable to a repeat of the same attack]. When a large-scale event takes place, these costs can be substantial:

When we were hit with the slammer virus, we lost on a worldwide basis all of our NT servers for email, applications, and database functionality. The entire company was unable to complete any office work for more than a week. Since the virus went into the directory services of the [operating system] software, we had to rebuild by hand EACH SERVER and we have hundreds of them. It took us a few days just to identify the problem and comprehend how it worked. Before doing anything to our infrastructure, we first had to develop a "patch," then test it thoroughly before using it. Finally, moving across our corporate network on a segment by segment basis, we got things up and running, but not before many trials and errors. I can't imagine how to calculate all of the total resources wasted in this event, but it was enormous.

Consequently, we can see that the interviewee described two types of costs: (a) the nightmare of rebuilding an extensive infrastructure, and (b) the loss of business productivity that was generated as a result. Unfortunately,
it is difficult to estimate the effects of temporary cut-offs of white-collar work, just as it is inherently difficult accurately to measure white-collar productivity.

PERSONNEL. It is said that more than 80% of Internet fraud [and related computer crime] is accounted for by either (a) "inside job" activities of your employees, or (b) mistakes. Other common problems are generated by (c) poor [or zero] training, or (d) compromised employees. Contrary to popular perception, resisting penetration by strangers from the outside represents only a small part of the total challenge.

Consequently, an organization usually must endure the following expenditures as a consequence of an event:

1. Termination and re-hiring of personnel.
2. Associated [usually litigation] costs with termination.
3. Associated [usually head-hunters or executive placement] costs with new hiring.
4. Probable salary differential [higher] for replacement personnel.
5. Re-training costs of new personnel.

III. USE IN VICTIM COMPENSATION

Victims of Internet fraud can be (a) governments, (b) institutions [including businesses], or (c) individuals. Consequently, the estimation of the cost of Internet fraud [and related computer crime] vary, and are based on different scales.

Regarding compensation for Internet fraud, we can make the following observations:

OBSERVATION 1. Due to the essential asymmetrical nature of Internet fraud, the perpetrator rarely has enough "deep pockets" if any at all against which and from which any significant compensation might be obtained.

Two years ago, a high school student in Malaysia released a computer virus. We picked it up in our subsidiaries in Asia, but were unable to stop it in Europe before it infected our North American operations. In
addition to our problems, that single incident cost U.S. corporations several billion dollars damage. Although he said he was “sorry,” from a practical point of view, there was no possibility of getting any type of meaningful compensation for the damages done.

This is a universal problem when seeking compensation for Internet based fraud, and there are at least two equally frustrating variations:

1. The perpetrator has no “deep pockets” from which recovery might be taken; or
2. It is impossible even to identify the perpetrator.

Another variation is that even if the above two factors do not interfere, international jurisdictional problems [e.g., extradition], make it impossible to take any meaningful action.

Observation 2. Each Internet fraud generates a series of cascading effects—primary, secondary, tertiary, etc.—and like any tort there is a point in the chain of causation where the effect becomes so remote that sure causation is arguable. The practical result of this is that ultimately, the settlement of any compensation or restitution issue is unlikely to be strictly related to the actual harm caused. Particularly when considering the intangible aspects of the problem, one would suspect that more likely than not calculated damages will be substantially less than actual.

This leads to several tentative conclusions regarding the calculation of the costs of Internet fraud [and related computer crimes] for the different parties that are victims, e.g., governments, institutions and individuals.

A. Government as Victim

We can identify at least two categories of government-related issues in Internet fraud [and related computer crimes].

Harm to Government. There are many examples of harm through Internet fraud to government. The principal and most serious threats include:
1. Espionage and theft of classified information;
2. Sabotage of vital government functions or services;
3. Anti-government dis-information and propaganda; and,
4. Penetration of government systems for the purpose of corrupting government decisions, including allocation of resources.

For the first class “Harm to Government” there is no point in estimating the value of the damage or the cost. All of the activities mentioned are well covered by Federal statutes or administrative practices. In addition, the government is well-staffed to protect its own interests since for all practical purposes it has almost unlimited manpower to counteract an Internet fraud should the occasion arise, e.g., if the damage or threat is great enough to merit a high level of attention.

**Criminal Prosecution.** It is the government—Federal, State & Local—that is tasked with exacting the judicial compensation society demands for this type of damage. In addition to the “standard” use of incarceration, damages are composed of:

1. Monetary fines.
2. Punitive damages.\(^{17}\)
3. Injunctive relief.

Generally, these punishments are determined by sentencing guidelines, containing fixed values. It appears that many fines are not calculated in relationship to the amount of damage, but rather are designed with end in mind of discouraging behavior.

Consequently, we can conclude that the entire class of damages from Internet fraud [and related computer crimes] as suffered by the government sector is not a relevant [useful] calculation [or estimation] to be made on a case-by-case basis.

\(^{17}\) Usually imposed for willfully abusive behavior on the part of the convicted defendant.
B. Institutions [including Businesses] as Victim

In contrast, when an institution [including businesses] are seeking compensation, then estimating the value of damages is crucial to the outcome. See Table 1 at the end of this paper where we have divided the types of cost estimations into three categories based on their immediacy to the criminal event.

PRIMARY TIER. These are cost effects felt immediately upon occurrence of the Internet fraud. For example, the theft of property is immediate. [It is “gone” simultaneously with the event.]

For this type of loss, the cost estimation may be based on the immediate replacement value of the items [property] taken.

SECONDARY TIER. These cost effects are suffered as an immediate consequence of the Internet fraud [or related computer crime]. The most important among these is the “Reputational Effect,” and as pointed out evidence indicates it can influence the stock market capitalization of the damaged victim firm.

Note that it is this effect and its possibly high or even fatal amount of damage that is at the root of the greatest executive fear, and explains the aversion to formal reporting [or other public disclosure] of any event.

TERTIARY TIER. Although virtually impossible to estimate, some thefts [or other Internet frauds] can cause long-term disruptions to the organization [or enterprise]. For example, the company might be completely precluded from entry into a market, thus losing potentially large amounts of revenue.

Due to the essentially speculative nature of these estimates [e.g., it is difficult to base the level of recoverable damages on a counting of future revenue that is only a possibility but not confirmed] we await a way to incorporate them into a grand tally of the cost of Internet fraud [and other related computer crimes].

For all practical purpose, it is not possible reasonably to estimate these costs.

---

18 This is very unfortunate, because the long-term effects of some Internet frauds are much more serious than are short-term effects, e.g., the company may be driven out of business.
C. Individuals as Victim

To most, horrible events in this category are criminal offenses involving homicide, soliciting, stalking, and sex crimes. The estimation of cost falls into the same category of anti-government [criminal] crimes, and thus is set not by calculation [or estimation] but by established schedules of penalties. In this context as well then, it not relevant to make an estimation.

However, for most crimes, there can be a civil tort complaint and the estimation of costs fall into the “classical” categories including (a) direct financial loss, (b) mental anguish, (c) damage to reputation, or (d) other types of damages associated with torts.

The rules governing tort recovery are more or less set and there is no need to review them here.

However, it should be added that it is likely that in contrast to institutions, individuals face generally severe and difficult hurdles achieving any compensation, and the standards required for showing of damages likely preclude real accommodation for the time and mental anguish spent in seeking compensation.

IV. CONCLUSION

This analysis suggests the following:

1. For criminal offenses, apart from punitive damages, the value of compensation for Internet fraud [and related computer crime] is fixed by sentencing [and other regulatory] guidelines; consequently, estimation of damages is not relevant.
   • NB: If such calculations were made for each event, they likely would differ substantially from agreed upon penalties.

2. For Internet fraud involving conversion of physical goods [e.g., inventory] or even most services, calculations of cost are straightforward, as they involve merely replacement or
substitution costs,
• NB: Usually any associated administrative costs are added to these numbers as it represents the costs of making the replacement.

3. For compromise of intellectual property, including trade secrets, estimation of the costs is speculative in nature, since it must rely upon forecasting of how the property probably would benefit the victim in the future.
  • NB: The result is that the value is "calculated" likely will be the result of negotiations between the payer and payee.

4. For any use of external services [e.g., lawyers, accountants, consultants, forensic data services, investigators, etc.] the value of the harm is easily calculated by simply adding up the bills.
  • NB: The opposite is true for those resources expended internally. Usually companies fail to keep track of this,
  • NB: The individual equivalent of this would be the mental anguish and time wasted in cleaning up the mess left by an Internet fraud crime.

5. The consequent changes in (a) organizational behavior [or procedures], (b) re-engineering of security related procedures and infrastructure, are easy to calculate, because in more or less all organizations, these are done under a disciplined budgetary procedure. These expenditures can be very significant.
  • NB: It is doubtful the bulk of these mandatory costs can be added to any damages award, and they are not reported in general computer crime statistics, but nevertheless they can be quite extensive, although “mixed” with other purposes.
Finally, it is important always to keep in mind the difference between (a) criminal penalties, (b) damage awards deriving from litigation, and (c) the true cost of Internet fraud [and related computer crime] which as you can see is likely much greater than either reported, or accounted for in litigation.
Table 1: Types of Cost Estimations for Internet Fraud [and Computer Related Crime]

Note: Use for Institutions and Individuals.

<table>
<thead>
<tr>
<th>Type of Loss</th>
<th>Suggested Estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRIMARY TIER</strong></td>
<td></td>
</tr>
<tr>
<td>Theft of Tangible Property</td>
<td>Value of Property + Administrative Costs of Recovery.</td>
</tr>
<tr>
<td>Theft of Services</td>
<td>Standard Value of Service if Purchased + Administrative Costs.</td>
</tr>
<tr>
<td>Theft of Trade Secrets</td>
<td>If in inventory, then use “book value” registered; if not recognized, then value is subject of negotiation.</td>
</tr>
<tr>
<td><strong>SECONDARY TIER</strong></td>
<td></td>
</tr>
<tr>
<td>Reputational Effect</td>
<td>Negotiated valuation; drop in capital valuation of company; drop in reasonably expected sales.</td>
</tr>
<tr>
<td>Administrative Recovery Expenses</td>
<td>Cost of extra expenses associated with terminating and resolving the incidence, including: (a) legal costs, (b) investigative fees, (c) management time, and (d) other consulting and advisory fees.</td>
</tr>
<tr>
<td><strong>TERTIARY TIER</strong></td>
<td></td>
</tr>
<tr>
<td>Competitive Displacement</td>
<td>Value of (a) permanent loss of market share, or (b) wind up value of company if driven out of business [by competition based upon using stolen trade secrets], or (c) estimation of opportunity cost for either (i) loss of geographical market, or (ii) inability to enter into new product line.</td>
</tr>
<tr>
<td>Security Administration (including Insurance)</td>
<td>Value of increased security costs [including additional insurance] compelled as a result of the Internet fraud incident including (a) staff turnover or extra hires, (b) re-engineering training and security awareness, and (c) purchase and operation of extra computer and network security infrastructure.</td>
</tr>
</tbody>
</table>

Source: Barracough Legal Research
Table 2: Types of Internet Crime and Estimation of Losses

<table>
<thead>
<tr>
<th>CRIME</th>
<th>ESTIMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANTI-INDIVIDUAL CRIMES</strong></td>
<td></td>
</tr>
<tr>
<td>Murder, Negligent Homicide, Soliciting</td>
<td>No significant difference with same</td>
</tr>
<tr>
<td>Suicide, Harassment, IIED, Stalking</td>
<td>crimes not committed via Internet.</td>
</tr>
<tr>
<td><strong>SEX CRIMES</strong></td>
<td></td>
</tr>
<tr>
<td>Soliciting a Minor, Corruption, Luring,</td>
<td>No significant difference with same</td>
</tr>
<tr>
<td>Misuse of Personal Information on Minor,</td>
<td>crimes not committed via Internet.</td>
</tr>
<tr>
<td>Sexual Harassment, Compelling</td>
<td></td>
</tr>
<tr>
<td>Prostitution, Pimping</td>
<td></td>
</tr>
<tr>
<td><strong>OPERATIONAL HARM</strong></td>
<td></td>
</tr>
<tr>
<td>Spamming, Denial of Service Attacks,</td>
<td>Restoration costs, investigation and</td>
</tr>
<tr>
<td>Vandalism, Release of Malware,</td>
<td>prosecution costs, loss of business,</td>
</tr>
<tr>
<td>Cybersquatting, Illicit Modification of</td>
<td>reputational loss, possible secondary</td>
</tr>
<tr>
<td>Files, Falsification of Files.</td>
<td>losses to third parties.</td>
</tr>
<tr>
<td><strong>MISUSE OF INTERNET</strong></td>
<td></td>
</tr>
<tr>
<td>Gambling, Selling Liquor or Cigarettes</td>
<td>Covered by regular penalties and</td>
</tr>
<tr>
<td>to Minors, Sale of illicit Prescription</td>
<td>damages. No significant difference</td>
</tr>
<tr>
<td>Drugs.</td>
<td>they are done via Internet.</td>
</tr>
<tr>
<td><strong>INFRASTRUCTURE DAMAGE</strong></td>
<td></td>
</tr>
<tr>
<td>Computer Trespass, Malware (virus attacks),</td>
<td>Cost of recovery &amp; repair; Loss of</td>
</tr>
<tr>
<td>Destruction of Data, Modification</td>
<td>Business; Reputational Loss; Change</td>
</tr>
<tr>
<td>or Corruption of Data, Denial of Service.</td>
<td>in Insurance Premiums.</td>
</tr>
</tbody>
</table>
FRAUD AND THEFT

| Change credit rating; Embezzlement; Theft of Information; Theft of Services; Computer Impersonation; Phishing; Theft of Goods; Theft of Money. | For Theft of goods and services, use market value; for change of credit rating, use value difference in additional credit obtained; For Impersonation, estimate damages caused [no damages if act had no result]. It is necessary to estimate the secondary effects of loss [e.g., misuse] of personal name-linked information. |

ANTI-GOVERNMENT CRIMES

| Obstruction, Failure to Report, False Reporting, Tampering with Evidence, Endangering Public Safety | Use accepted criminal penalties. No significant difference because crimes committed with Internet. |

THEFT OF INTELLECTUAL PROPERTY

| Stealing of Patents; Improper use of Copyrighted Material; Theft of Trade Secrets. | For patent infringement, use standard remedies and values. Same for Copyrighted materials that are taken. For Trade Secrets, it is problematical to assign a value since (1) values may change over time, (2) many values are of necessity “speculative” in nature. |

Based on the Model Computer Crime Code