Faking It: Calculating Loss in Computer Crime Sentencing

JENNIFER S. GRANICK*

ABSTRACT

This paper argues that the sentences courts have been imposing for violations of the federal computer crime statute – 18 U.S.C. § 1030 – do not accurately reflect the seriousness of the offense or treat like offenders equally. By definition, sentencing is heavily dependent on economic measures of harm, particularly the cost of investigating the incident and restoring the system to its original state. The legal definition of harm, however, does not accord with the real world responses of investigators who want to get critical systems running again to improve the state of security. Also, by focusing on monetary loss, sentences do not adequately reflect intangible damage that is difficult to value monetarily, like invasions of privacy, access to or theft of data, or interruption of service. The readily measured monetary loss like labor and hardware costs associated with investigating, repairing, and restoring compromised systems are more a function of victims' choices than a reflection of perpetrator wrongdoing or system interference. Sentencing law and practice has failed to discriminate between harmful and trivial attacks. There are several legal approaches we could adopt to mitigate these problems. Ultimately, the question of how to remedy intrusions depends on whether a consensus evolves about the value of the rights and property interests that are commonly harmed by computer attacks.

INTRODUCTION

This paper argues that the sentences courts have been imposing for violations of the federal computer crime statute – 18 U.S.C. § 1030 – do not accurately reflect the seriousness of the offense or treat like offenders equally. The problem arises for both doctrinal and practical reasons. By definition, sentencing is heavily dependent on economic measures of harm, particularly the cost of investigating the incident

---

* Jennifer Stisa Granick joined the faculty of Stanford Law School in January 2001, teaching the Cyberlaw Clinic and acting as Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues, including computer crime and security, national security, constitutional rights, and electronic surveillance–areas in which her expertise is recognized nationally.

and restoring the system to its original state. But the legal definition of harm does not accord with the real world responses of investigators who want to get critical systems running again to improve the state of security. Also, by focusing on monetary loss, sentences do not adequately reflect intangible damage that is difficult to value monetarily, like invasions of privacy, access to or theft of data, or interruption of service. The readily measured monetary loss like labor and hardware costs associated with investigating, repairing and restoring compromised systems are more a function of victims' choices than a reflection of perpetrator wrongdoing or system interference. Moreover, victims with more critical systems tend to spend little time investigating the intrusion and a lot of time improving security and getting the affected machines back on line. Sentencing law excludes expenses incurred for both practices. Meanwhile, victims with less important systems have the luxury of time to conduct a full forensic investigation, which ratchets up prison terms. Thus, sentencing law and practice has failed to discriminate between harmful and trivial attacks.

There are several legal approaches we could adopt to mitigate these problems. Obviously, courts could take practical steps to ensure that victims do not overstate the economic costs of remediation, including requiring accurate and complete documentation from victims. Raising the burden of proof at sentencing would encourage this practice. Another answer might be to reduce the weight given to economic loss and more heavily weigh factors like the number of victims, nature of information accessed by the attacker, nature of the system attacked, or criminal scienter. The sentencing guidelines have started down this path by adding sentencing adjustments to reflect the number of victims, interference with critical infrastructure, and the like. But, adding adjustments will not fix the problem if economic costs continue to weigh so heavily in the sentencing process. Sentences will still be unfair and unequal, however; they will just be more severe. Ultimately, the question of how to remedy intrusions depends on whether a consensus evolves about the value of the rights and property interests that are commonly harmed by computer attacks.

MEASURING ECONOMIC LOSS IS FUNDAMENTAL IN COMPUTER CRIME CASES

Computer crime sentencing requires courts to value the damage caused by a computer intrusion. In 2005, U.S. Supreme Court decisions in *United States v. Booker* and *United States v. FanFan*[1] changed the way federal courts sentence in criminal cases. The decisions stem from prior case law holding that a defendant has a right to trial by jury for any factor that increases the defendant's sentence.[2] *Booker* and *FanFan* then held that the United States Sentencing Guidelines, to the extent that they are mandatory, violate the Constitution when the total offense level upon which the trial court sentences include aggravating factors not found to be true beyond a reasonable doubt by a jury.[3] A different majority of the Court then held that the Guidelines are acceptable so long as they are not mandatory.[4] Courts are free to be guided by the Guidelines but need not sentence in accordance with them, and sentencing decisions will be reviewed for "reasonableness."[5] The amount of harm a defendant caused is relevant to sentencing courts. Courts will calculate that harm in accordance with both statutory and Guideline definitions.

The Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030, prohibits unauthorized access to computer systems.[6] Damage, expressed in terms of monetary loss, is important in computer crime cases in three ways: (1) it is an element of the crime; (2) it is a major determinative factor in sentencing; and (3) it is fundamental to restitution. While the statute clearly contemplates intangible harms from unauthorized access to data and systems, it requires fact finders to express those harms in economic terms.

---

[1] United States v. Booker, United States v. FanFan, 543 U.S. 220 (2005) (case opinions are combined).

[2] Apprendi v. New Jersey, 530 U.S. 466 (2000); Blakely v. Washington, 542 U.S 296 (2004).

[3] Booker, FanFan, 543 U.S. at 245. (Justice Stevens wrote the Court's opinion on this issue, with Justices Scalia, Souter, Thomas, and Ginsburg joining.)

[4] *Id.* at 259. (Justice Breyer wrote the Court's opinion on this question, with the Chief Justice and Justices O'Connor, Kennedy, and Ginsburg joining.)

[5] *Id.* at 263-264.

[6] 18 U.S.C. § 1030 (2005).

Prior to 2001, section 1030 focused almost exclusively on economic harm from damage to computers and computer systems. Subsections (a)(1)-(4) have not been amended. Subsection (a) of the statute addresses unauthorized access to classified information. Subsection (a)(2) makes unauthorized access and obtaining any information from a protected computer criminal, but is only a misdemeanor. Subsection (a)(3) criminalizes access that interferes with the ability to use a computer exclusively for government use. Subsection (a)(4) criminalizes access with the intent to defraud if the intruder obtains anything of value. Prior to the 2001 amendments, subsection (a)(5) criminalized transmissions or access that caused damage, where damage was defined as any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating to at least $5000 to one or more person during any one-year period as an element of the offense.[7] Without sufficient loss, there was no offense under (a)(5). For access to private systems, the statute required a showing of economic harm, or else, the offense was a misdemeanor.

The statute generally defines damage as including interference with the integrity of the system and then gives specific examples of more tangible losses, including "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[8] Thus, loss is a critical element in defining whether a crime has occurred.

Amendments to the statute in 2001 added some special kinds of non-economic harm that could substitute for showing $5000 in loss. The non-economic harms are:

> the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; [access that causes] physical injury to any person; a threat to public health or safety; or damage affecting a computer system used by or for a government entity in furtherance of the

---

[7] 18 U.S.C. § 1030(a)(5)(B)(i).

[8] 18 U.S.C. § 1030(e)(11).

> administration of justice, national defense, or national security.[9]

A few years after these amendments, in 2004, the United States Sentencing Commission issued new sentencing guidelines with adjustments for violations creating these non-economic harms. However, as discussed below, the adjustments are minor add-ons contemplating that the largest factor in computer crime sentencing will remain economic loss.

Prior to 2005, the United States Sentencing Guidelines (Guidelines) regulated all federal criminal sentencing. The Guidelines were promulgated by the U.S. Sentencing Commission at the behest of Congress to limit judicial discretion and impose order on federal sentencing across districts. The Guidelines establish a base offense level (BOL) for various crimes, and then list various factors that increase or decrease the sentence (generally called adjustments). Once the sentencing court determines the total offense level, taking all the mitigating and aggravating factors into consideration, and considers the defendant's prior criminal history, the Guidelines prescribe a period of incarceration.[10] In the absence of extraordinary circumstances, the sentencing court must choose a sentence within the narrow range of months of incarceration the Guidelines prescribe.

Economic loss is a major factor in computer crime sentencing under the Guidelines. For the purposes of sentencing, loss is defined in the same economic terms as under the statute. That monetary value is then heavily weighted in sentencing. Section 2B1.1 of the Guidelines applies to CFAA violations. Section 2B1.1 has a BOL of six and dictates a two to thirty level upward adjustment for loss.[11] If loss is $30,000, the loss adjustment is six levels. Thus, at $30,000 loss or more, over half of the defendant's sentence may be determined by loss alone.[12]

---

[9] 18 U.S.C. §§ 1030(a)(5)(B)(ii)–(v).

[10] 28 U.S.C. § 994(a) (2005).

[11] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(1)(D) (2005) [hereinafter U.S.S.G.].

[12] The BOL for violations of 18 U.S.C. § 1030 that do not involve state secrets is six (6). U.S.S.G. § 2B1.1(a)(2). The Guidelines add an additional six (6) levels for loss greater than $30,000, and continue increasing up to an additional thirty (30) levels. Since the maximum sentence for a first time violation of 18 U.S.C. § 1030 is ten years, you can get the maximum at a level thirty, or a loss of $50,000,000 without any other aggravating factors.

Finally, the amount of economic loss directly affects restitution orders. Under non-mandatory restitution provisions, the court is to consider the amount of the loss sustained by each victim as a result of the offense.[13] In the case of an offense that damages or causes loss to property, the statute requiring mandatory restitution requires defendants to pay:

> the greater of--
>
> (i) the value of the property on the date of the damage, loss, or destruction, or
>
> (ii) the value of the property on the date of sentencing, less the value (as of the date the property is returned) of any part of the property that is returned . . . [14]

Defendants also must "reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense."[15] The federal code establishes a procedure whereby the U.S. Probation Department collects evidence from victims, prosecution, and defense about the appropriate amount of restitution.[16] Whatever restitution scheme applies, sentencing courts are obligated to put a monetary value on the harm from the offense and to receive input, either directly or indirectly, through the probation department from both the government and the defendant.

Statutory and Guideline definitions require economically expressible losses for prosecution and punishment of computer intrusions. As courts look to the cost of investigation and remediation as a measure of a defendant's guilt, cases involving intangible harms,

---

[13] 18 U.S.C. § 3663 (2005).

[14] 18 U.S.C. §§ 3663(b)(1)(B)(i)–(ii).

[15] 18 U.S.C. § 3663A(b)(4). At least one court has held that restitution following conviction of 18 U.S.C. § 1030 is mandatory under 18 U.S.C. § 3663A. *See* United States v. Harris, 302 F.3d 72, 75 (2d Cir. 2001) (holding that restitution following conviction of 18 U.S.C. § 1030 is mandatory under 18 U.S.C. § 3664A(b)(4)).

[16] 18 U.S.C. § 3664(a).

but no economic losses, are unlikely to be pursued. Thus, invasions of victim privacy, for example, will not be prosecuted unless the victim can come up with additional economic harms. Section 1030 provides a civil remedy for victims, and in several cases, victims have failed to obtain redress because harm to their privacy interests was not economically calculated to exceed $5000.[17]

In 2004, the Guidelines were amended to include a number of upward adjustments for non-economic factors. These include number of victims,[18] misappropriation of a trade secret with the knowledge or intent to benefit a foreign government,[19] the conscious or reckless risk of death or serious bodily injury,[20] attacks on critical infrastructure or national security machines,[21] and violations with the intent to obtain personal information.[22] Given the recency of these amendments and the current confusion over the status of the sentencing guidelines, there has been little data to determine the effect of these changes. However, loss still remains the single, overwhelmingly important factor. Economic loss can add anywhere from a minimum of two to a maximum of thirty levels to a sentence.[23] The non-economic factors, however, generally result in an upward adjustment of only two levels, and in serious cases involving interference with critical infrastructure systems, six levels, but no more.[24]

---

[17] For example, plaintiffs have filed class action suits against companies that place "cookies" on the computers of website visitors for the purpose of collecting private data for marketers. While the courts have found that cookies are an unauthorized access to computers in violation of the actus reus provisions of § 1030, the invasion did not cause $5000 in loss and thus dismissed the suit. *See* In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1791 (C.D. Cal. 2001) (Plaintiffs failed to show that privacy invasion was an economic loss in the amount of $5000 or show non-economic damage of the type listed in 18 U.S.C. §§ 1030(e)(8)(B)–(D)).

[18] U.S.S.G. §§ 2B1.1(b)(2)(A)–(C) (2005).

[19] U.S.S.G. § 2B1.1(b)(5).

[20] U.S.S.G. § 2B1.1(b)(12)(A).

[21] U.S.S.G. § 2B1.1(b)(14)(A)(i)(I).

[22] U.S.S.G. § 2B1.1(b)(14)(A)(i)(II).

[23] U.S.S.G. § 2B1.1(b).

[24] U.S.S.G. § 2B1.1(b)(2), (5), (12), (14).

COMPUTER INVESTIGATION COSTS ARE A FUNCTION OF VICTIM CHOICE, NOT OFFENSE CONDUCT

Incident investigation costs are clearly included in the statutory definition of loss. Following a security breach, owners incur labor costs for investigating the incident and fixing the vulnerability that allowed unauthorized access. Owners may also incur labor and hardware costs for upgrading or improving security measures like firewalls and intrusion detection systems. Investigation costs should be easily measured if the owner documents the activities responders take and the hardware they use.

Despite the apparent ease of measurement, victims faced with nearly identical security incidents will tally different losses. The reason for this is that there is no one right way to do security incident investigation. Victims' goals affect investigation decisions. Victims may decide to restore a mission-critical machine to service with a cursory investigation that adds up to little economic loss.

Also, victims can over- or under-report the cost of conducting an investigation. Victims who want federal assistance in investigating or prosecuting an attacker know that the higher the loss, the more likely the Federal Bureau of Investigation (FBI) will be interested. Victims may choose an expensive investigation to reassure shareholders or the public and to restore their reputation for security.

Security incident investigation is something of an art, and investigations performed by different technicians will not take anywhere near the same amount of time or resources. In 2001, the Honeynet Project hosted a forensic challenge, publishing an image reproduction of a compromised system, and challenged contestants to analyze the attack and report what they found.[25] The contestants were told to keep track of their time and were given the federal statutory definition of loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[26]

---

[25] The Forensic Challenge, http://www.honeynet.org/challenge/ (last visited Oct. 26, 2005).

[26] *Id.* (referencing Dave Dittrich, *Estimating the Cost of Damages Due to a Security Incident*, (Jan. 29, 2001) *available at* http://staff.washington.edu/dittrich/misc/faqs/incidentcosts.faq.)

Participants were also instructed to assume that their annual salary was $70,000.[27]

The challenge received thirteen entries. The consensus was that the analysis of this single-compromised system took quite a bit of time. Contestants finished when the contest time ran out, not when they were done. The average time spent per investigation was forty-eight hours.[28] The most time spent was 104 hours.[29] The least was ten.[30] The winning entry took thirty-seven hours and was submitted by a single investigator with eight years of experience.[31] At the $70,000 salary, the average cost per investigation was approximately $2000.[32]

What these contest results show is that the cost of fixing a system after an attack has more to do with what actions the victim takes than with what the intruder did. Damage from an offense is a function of the idiosyncrasies of incident investigation, including the skills, experience, hourly rate, and remediation choices of the victim, and not necessarily the offender's actions. As a result, similar offenders committing similar offenses will be treated differently, because victims will inevitably react differently to intrusions.

Beyond victim idiosyncrasies, intrusion response depends on the victim's goals. The victim may want to perform a thorough analysis of the incident to determine what happened and to learn from the problem. He or she may want to perform a thorough analysis of the incident for use in a legal case against the perpetrator. Or more pressingly, the victim may want to get the computer systems back up and running as quickly as possible to avoid business losses. Doing a full-scale analysis for any purpose may interfere with restoring

---

[27] The Forensic Challenge, *supra* note 25.

[28] The Forensic Challenge, *Results of the Forensic Challenge*, http://www.honeynet.org/challenge/results/index.html (last visited Oct. 26, 2005).

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

services. The expense of identifying a perpetrator, versus putting the services back on line, can be immense.[33]

The intrusions that took place in *United States v. Butler*[34] illustrate this point exactly. In *Butler*, I represented a man who created an automated tool that used a known vulnerability to compromise systems and install new codes that both patched the known vulnerability and installed an unknown back door through which he could regain access. Each system accessed by his tool was accessed in exactly the same way, since the tool used an identical automated process on each machine. Some system administrators restored their machines from backup and reported a single hour of work. At government pay rates, this was far less than the requisite $5000 of loss. Other system administrators reported spending over thirty hours examining the compromised machines, as well as examining other machines that were not compromised, to investigate the attack. Here, the costs were well above the $5000 threshold.[35] The loss Butler caused could be aggregated across machines as part of a similar course of conduct. However, if Defendant A had compromised the first system and Defendant B the second in identical ways, but unrelated incidents, Defendant A would not be prosecuted, but Defendant B would go to prison.

A system owner who decides to investigate will rack up more losses in the form of labor costs than a system owner who decides that the computers are mission-critical and have to be put back on line immediately. As a result, the first incident will be punished more harshly than the latter, though arguably the intrusion into the mission-critical system was more disruptive than an attack on a system where the owner had the luxury of time to investigate.

Not only is the decision of whether to investigate often inversely related to the importance of the attacked system, it also may be based

---

[33] *See* NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUBL'N NO. 800-61, COMPUTER SECURITY INCIDENT HANDLING GUIDE (2004) § 3.3.3, *available at* http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf. ("Identifying the attacker can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact.") [hereinafter NIST GUIDE].

[34] United States v. Butler, No. CR00-20096 JW/PVT (N.D. Cal. filed Mar. 15, 2000) (Sentencing hearing held on May 24, 2001).

[35] *Id.;* Defendant's First Amended Sentencing Memorandum Motion for Departure Request for Evidentiary Hearing, United States v. Butler, at 25 (filed May 14, 2001) (on file with author).

on efforts to remediate harm to a company's reputation rather than to its computer systems. For example, in *United States v. Heckenkamp*,[36] the defendant was accused of altering an Internet auction site, eBay's webpage. eBay had hired several expensive consulting firms to investigate its website intrusion. Even though replacing the altered page with the original is a simple process, the publicly traded company probably felt it needed to do more to build customer confidence.[37] Potential harm to reputation caused the company to spend a lot more on remediation and upgrades to reassure its customers and the public than it otherwise would have done. Generally, U.S. law does not compensate harm to reputation resulting from the publication of true facts. If harm to reputation stems from the public realization that the system was not, in fact, secure, or from public revelation of information that makes a company look bad, the legal system may not want to factor this specific injury into sentencing. But harm to reputation also influences how much time and money a victim will spend on remediation. Courts that defer to victim loss assessments will have trouble excluding harm to reputation from sentencing considerations.

When different victims treat an identical attack differently, vastly disparate loss calculations result, and thus sentences vary as well. The victim's choice about how to respond to a security incident is the difference between innocence and prison, despite the fact that the unauthorized access was exactly the same.

The judicial system often imposes liability on similar offenders based on events outside of the perpetrator's control that are nonetheless proximately caused by the illegal conduct. If I punch someone, I have committed a battery. But if that person falls and hits his or her head and dies, I can be prosecuted for manslaughter. In computer crime prosecution, the difference is stark because of the $5000 trigger for liability and the relatively steep increase in offense level proscribed by the relevant sentencing guideline.[38]

---

[36] United States v. Heckenkamp, No. 00-CR-20355 JW/ALL (N.D. Cal. filed Dec. 13, 2000) (case terminated by plea and sentence April 27, 2005). A summary of this case is available on the Dep't of Justice, Computer Crime and Intellectual Property Section website as a press release, http://www.usdoj.gov/criminal/cybercrime/heckenkampSent.htm.

[37] *Id.*

[38] A defendant can go from zero to sixteen months in $30,000. U.S.S.G. § 2B1.1, and Ch.5, Part A (Sentencing Table) (2004).

Moreover, victims generally have incentives to mitigate harm flowing from the illegal act. Few people want to make their injuries worse. But victims who choose an expensive full-scale investigation do not necessarily pay a penny more than victims who restore from backup and put their systems back on line. In-house investigators get the same yearly salary regardless of the choice. Indeed, there may be an incentive to exaggerate. If the victim can portray the incident as serious, federal law enforcement is more likely to get involved in the investigation. Victims who inflate the number of hours spent on remediation can end up saving money by shifting real investigation and prosecution costs to the taxpayer.

Thus, the most easily measurable type of harm that accrues from a computer attack is both unrelated to the severity of the intrusion and subject to manipulation by victims. As a result, investigation costs do not correlate with the invasiveness or disruptiveness of attacks.

INVESTIGATION ACTIVITIES FALL OUTSIDE THE LEGAL DEFINITION OF LOSS

Courts have good cause to look more closely at victim loss estimates because they tend to include losses that are excluded by law. Despite the importance of "loss" in computer crime cases, the factor is defined in a way that does not accord with the real-world effects of computer crime. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[39] Loss does not include any costs incurred improving the system, nor does it include costs for forensic investigation.[40] The comments to the relevant Guideline 2B1.1 expressly exclude forensic costs, i.e. "costs to the government of, and costs incurred by victims primarily to aid the government in, the prosecution and criminal investigation of an offense."[41]

---

[39] 18 U.S.C. § 1030(e)(11) (2005).

[40] *See* United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000) (the finder of fact could consider only those costs that were a "natural and foreseeable result" of the defendant's conduct, that were "reasonably necessary," and that would "resecure" the computer).

[41] U.S.S.G. § 2B1.1, cmt. n.3(D) (2005).

First, no victim wants to put the system back into its original condition. Everyone wants to improve. Incident handlers do not restore a compromised system to its "condition prior to the attack" as contemplated by the definition. Prior to the attack, the system was vulnerable. The administrator is going to improve the security of the system so that the same attack will not be successful the next time. Responders "harden" systems, install patches, and tighten network perimeter security.[42]

Second, victims invariably include forensic costs as part of labor in response to an intrusion. First responders are taught to do a forensic investigation if at all possible, even though the legal definition of loss excludes forensic costs. Private and public organizations have developed standards and training programs for these first responders. For example, the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST) publish the "Computer Security Incident Handling Guide," which explores policies and practices that public agencies and private sector businesses should take following an attack.[43] The federally funded CERT Coordination Center (CERT/CC) also publishes resources for private organizations to build their own computer security incident response teams and to train incident handlers. Its October 2005 publication, "State of the Practice of Computer Security Incident Response Teams (CSIRTs)," is a review and digest of the top incident handling resources.[44] It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues.

The training manuals stress the importance of investigating incidents so that the information can be used in a subsequent civil or criminal case. Obviously, the Department of Justice (DOJ) guide is intended for law enforcement and for first responders to computer crime scenes. The entirety of the manual advises following appropriate forensic procedures with the intention of preserving evidence for criminal prosecution.

---

[42] If the intruder obtained passwords, changing passwords might be required to re-secure the system as a result of the incident.

[43] NIST GUIDE *supra* note 33.

[44] *See* Georgia Killcrese et al., *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (Oct. 2003) *available at* http://www.cert.org/archive/pdf/03tr001.pdf.

The NIST Guide, however, is targeted to all first responders, not only law enforcement and crime scene responders.[45] It is characteristic of the training that first responders receive in the public and private sectors.[46] First responders are told to collect evidence in a way that will hold up in court.

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies, so that it should be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence.[47]

The NIST Guide also recommends that the incident handler have forensic training so that she is familiar with legal rules and proceedings.[48] The Guide advises recovery actions, including "restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists)."[49] It also advises investigative actions, including validating the attacker's IP address, scanning the attacker's systems, performing web

---

[45] NIST GUIDE *supra* note 33 at § 1.3 at 1-1 ("This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), and computer security program managers who are responsible for preparing for, or responding to, security incidents.").

[46] The NIST document was based on the advice of security experts at NIST, consulting firm Booz Allen Hamilton, NASA, Indiana University, Center Education and Research in Information Assurance and Security (CERIAS), Purdue University, The U.S. Department of Veterans Affairs, Wells Fargo Bank, The University of Tulsa, CERT®/CC, MITRE Corporation, The Ohio State University, Lawrence Berkeley National Laboratory, The Federal Computer Incident Response Capability (FedCIRC), and U.S. Dep't of Treasury.

[47] NIST GUIDE *supra* note 33 at § 3.3.2 at 3-18.

[48] *Id.* at 3-19.

[49] NIST GUIDE *supra* note 33 at § 3.3.4 at 3-21.

research on attacker handles or email addresses, searching incident databases, and monitoring the attacker's electronic communications.[50]

Thus, system administrators are trained to contemplate either a criminal or civil action at the outset of the investigation. The guides recommend time-consuming system review and evidence preservation activities, which are useful only for legal cases. Procedures for documenting how evidence has been preserved, collecting evidence in accordance with laws and regulations, keeping chain of custody forms, communicating with legal counsel, and interviewing witnesses, all are part of building a legal case, not merely investigating what happened.

Forensic activities and training increase both the time spent by and the hourly cost of the incident handler, despite the legal exclusion of such costs.

This would not be a problem if courts scrutinized victim loss estimates. However, courts are highly deferential to victims. A review of the Department of Justice's selected computer crime cases, published at http://www.cybercrime.gov, shows thirteen cases sentenced in 2003 and 2004.[51] The information provided for six of the thirteen cases includes both the government's statement of loss and the court ordered restitution.[52] In four of the six cases, the fine or restitution order equaled or exceeded the government statement of loss, indicating that the court adopted the government's loss estimate.[53] In one of the other two cases, the government's stated loss was $100,000 and the court ordered $88,253.47 in restitution.[54] In the

---

[50] NIST GUIDE *supra* note 33 at § 3.3.3 at 3-20, 21.

[51] Dep't of Justice, Computer Crime and Intellectual Property Section, Table of Computer Intrusion Cases, http://www.usdoj.gov/criminal/cybercrime/cccases.html (last visited October 26, 2005).

[52] *See id.* (The six cases are *United States v. Borghard*, *United States v. Dinh*, *United States v. Ivanov*, *United States v. Shakour*, *United States v. Amato* and *United States v. Heckenkamp*, which have press releases summarizing the cases on the Dep't of Justice, Computer Crime and Intellectual Property website cited *supra* note 51.)

[53] *See id.* (These four cases are *Borghard*, *Dinh*, *Amato*, and *Heckenkamp*.)

[54] *See id.* (This case was *Shakour*.)

other, the government's estimated loss was $25 million, but the court ordered no fine or restitution.[55]

Courts could be less deferential if they had the documentation necessary to parse through the time spent or the hourly rate to try to excise extra costs motivated by forensic purposes. Unfortunately, investigating FBI agents do not ask victims to keep track of their time with the legal definitions of loss in mind. As a result, victims usually submit to courts undifferentiated loss estimates with few sub-categorizations that would aid a court in distinguishing between permissible and impermissible loss inclusions. Victims simply are not given the information necessary to avoid excessive loss calculations.

There is little or no incentive or format in which the victim can estimate damages in a legally useful way. For example, in *United States v. Butler*, the Air Force Office of Special Investigations (AFOSI) investigated the intrusions into Air Force computers. That investigation led to the identification of Butler as the perpetrator. The Special Agent in charge provided the FBI with a flat number of investigative hours the AFOSI devoted to the case. He provided no supporting documentation, list of type of work done, or records of when the work was performed. For sentencing, the government obtained another document from AFOSI detailing the work. The total number of hours on the worksheet was different from the number initially reported. Again, it contained no indication of what work was done. There was, therefore, no way to tell whether the calculation included time spent on activities explicitly excluded from the loss calculation. The court, nonetheless, sentenced Mr. Butler based on this information because it was a "reasonable" calculation.[56]

THE BURDEN OF PROOF AT SENTENCING IS TOO LOW TO INCENTIVIZE JUDGES TO TAKE A SERIOUS LOOK AT LOSS ESTIMATES BY VICTIMS

It is unsurprising that sentencing courts defer to prosecution and victim loss estimates. Judges do not have the expertise to second-guess a victim's assessment of what was required to investigate and fix his system. As the Honeynet data suggests, experts in the field can

---

[55] *See id.* (This case was *Ivanov*. A more in depth analysis of the data on computer crime sentencing is needed to confirm whether this assertion that courts are extremely deferential is true.)

[56] United States v. Butler, *supra* note 34.

differ widely over the proper course of an investigation.[57] Judges have little competency to question those decisions. However, the parties could bring in experts to support and attack the loss estimate and courts could make judgments based on testimony, as they do in other areas of the law. The burden of proof at sentencing and the standard of review on appeal are so low, especially now that application of the Guidelines is discretionary, that trial courts feel confident that any reasonable decision will be upheld.

The Guidelines do not limit loss in computer crime cases to foreseeable damages. While the definition of loss for other white collar fraud crimes punished under the same guideline includes only reasonably foreseeable monetary harm,[58] a special rule for computer crime cases requires the court to include any reasonable cost to any victim, "including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service," regardless of whether the harm was reasonably foreseeable or not.[59]

Also, the Guidelines establish a lower burden of proof for loss calculations in sentencing. Generally, the burden of proof required for sentencing is by a preponderance of the evidence.[60] However, the Guidelines only require the judge to make a "reasonable estimate" of the loss.[61] In other words, the government only needs to show by a preponderance of the evidence that the sentencing court made a reasonable estimate of loss, and that estimate is a factual finding entitled to great deference.[62]

Loss will continue to be a critical factor in sentencing decisions; however, courts will still be under little or no pressure to scrutinize

---

[57] *See*, The Forensic Challenge, *Results of the Forensic Challenge*, *supra* note 28. The competing teams performed very different incident analyses.

[58] U.S.S.G. § 2B1.1, cmt. n.3 (2005).

[59] U.S.S.G. § 2B1.1, cmt. n.3(a)(v)(III).

[60] *See, e.g.*, United States v. Hull, 160 F.3d 265, 269 (5th Cir. 1998); United States v. Collins, 109 F.3d 1413, 1420 (9th Cir. 1997).

[61] *See* U.S.S.G. §2B1.1, cmt. n.3.

[62] *See* 18 U.S.C. § 3742(e)–(f) (2005).

loss estimates, because the overall sentence only needs to be reasonable.

COMPUTER INTRUSIONS ARE CHARACTERIZED BY INTANGIBLE HARM NOT READILY QUANTIFIABLE IN ECONOMIC TERMS

Much of the harm flowing from computer intrusions is even harder to evaluate. Loss of privacy, access to confidential data, system unavailability or downgrade in system performance, and sometimes the revelation of previously unknown information all harm victims. The harm can be non-economic and may not require the victim to make any financial expenditure.

It is difficult to put a price tag on the harm caused when once private data is no longer secret. For example, I am adversely affected by knowing that an intruder, whether a stranger or someone I know, read my email without my permission. Information I wanted to keep private no longer is. There is a chance that the intruder will use the information against me in some way or that it will be embarrassing. Some victims of privacy invasion describe a psychological sense of violation. Yet there is no amount of money that would repair this harm. Money cannot make the victim whole.

Even where information is commercially valuable, unlike the email in the above example, there may be no readily measurable economic loss when an outsider merely accesses the information. Customer lists, trade secret information, or software programs under development may have no readily ascertainable market value. It is unclear whether that value diminishes if the owner of the information retains the full ability to exploit it following unlawful access, for example when an intruder learns of company trade secrets, but does not disseminate them further. In the case of *United States v. Mitnick*,[63] the defendant accessed proprietary data stored on Sun Microsystems computers. Sun claimed that Mitnick caused $80 million in damages by copying the source code for its Solaris operating system. This number represented the entire research and development costs for Solaris.[64] Yet, Mitnick did not disseminate the source code, and Sun was able to retain complete control of the product, later deciding to give the operating system to customers for free.

---

[63] United States v. Mitnick, 145 F.3d 1342 (9th Cir. 1998).

[64] Douglas Thomas, *How Much Damage Did Mitnick Do?*, WIRED NEWS, May 5, 1999, http://wired-vig.wired.com/news/politics/0,1283,19488,00.html.

Did Mitnick cause Sun no damage because he simply copied something that they were giving away for free, or did he cause $80 million in damage? Clearly, a trade secret does not necessarily lose all value to the owner simply because it is no longer secret from the attacker. Equally clear is that the victim suffers some harm from loss of total secrecy. The owner does not know how far the secret was disseminated and experiences some amount of uncertainty as to the continuing viability of the secret nature of the information. But, that uncertainty is not a kind of harm that is readily expressed monetarily.

In January and February of 2000, attacks took down several major webpages, including Yahoo!.[65] Yahoo!, which makes money from advertising, was down for several hours but was eventually restored. Yahoo! failed to display ads to its users during that time period, but did it lose any revenue? Would the attacker have been criminally responsible if an advertiser cancelled a million dollar contract with Yahoo! as a result of learning that the site was not immune to such attacks?

These difficult questions simply illustrate that the damages characteristically caused by computer intrusions are not readily expressed in economic terms.

Given the theoretical problems with converting intangible harm to economic losses, it is not surprising that individuals, businesses, and the government have trouble calculating the cost of computer intrusions or computer viruses. The problem is exacerbated because legal doctrine, government agencies, and private industry have not developed any guidelines or methodologies for making such estimates. When asked to measure harm from computer intrusions, victims are not given any guidelines or methodologies with which to do so. The Computer Security Institute (CSI) and the Federal Bureau of Investigation survey CSI members every year about a host of security issues, including number of security incidents and their cost. This report is the only one of its kind and is widely cited by media and industry. There are statistical and methodological problems with the survey that others have identified.[66] But for the purposes of this paper, one of the most interesting findings is that survey respondents have

---

[65] Corey Grice, *How a Basic Attack Crippled Yahoo*, CNET NEWS.COM, Feb. 7 2000, http://news.com.com/2100-1023-236621.html.

[66] *See, e.g.*, Julie C.H. Ryan & Theresa I. Jefferson, *The Use, Misuse, and Abuse of Statistics in Information Security Research*, Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

trouble figuring out how to quantify loss. The 2004 survey, as in other years, showed that almost half of the organizations were unable or unwilling to quantify financial losses.[67] A much higher percentage of 2005 survey respondents were able to estimate financial losses. Interestingly, the 2005 loss estimates were substantially lower than those in 2004, a "whopping 61% decline," [68] which CSI attributes to accurate measurements of explicit losses like the cost to reconfigure and reinstall software, but the difficulty in calculating implicit harm like lost revenue.[69] Nonetheless, the media seems to trade in undocumented assessments of economic loss which, to even the least critical reader, are suspiciously high. For example, news outlets widely reported the mi2g consultancy firm's estimate that January 2004's "mydoom" virus cost businesses $38.5 billion worldwide.[70]

Computer intrusions cause harm, but neither the legal system nor industry understands how to measure that harm. By insisting on an economic measure of harm, sentencing is too malleable by both victims and law enforcement. Meanwhile, harm from system malfunction, data loss, or privacy invasion goes under-punished.

Recent Guideline amendments providing upward adjustments for multiple victims, invasions of privacy, theft of trade secrets, and interference with government functionality or critical infrastructure may be a step in the right direction. By identifying aggravating offense characteristics without reference to money, sentencing law can better address intangible harms. But the current scheme only imposes these adjustments on top of the previously existing adjustments for financial loss. Adding adjustments will not fix the problems set forth above. Sentences will still be unfair and unequal. In addition, intangible harm will still be undervalued. For example, under the current Guidelines, "intent to obtain personal information" results in only a two-level increase, as does the theft of a trade secret for a

---

[67] CSI/FBI Annual Survey (2004), at 11, CSI/FBI Annual Survey (2005), at 2, 14. In 2004, 494 respondents, only 269 provided loss estimates. In 2005, of 700 respondents, 639 provided loss estimates. The survey is available at no cost from http://www.gocsi.com.

[68] *Id.* at 14.

[69] *Id.* at 15.

[70] mi2g Ltd., *My Doom Becomes Most Damaging Malware as SCO Is Paralysed*, Feb. 1, 2004, http://www.mi2g.com/cgi/mi2g/press/010204.php.

foreign agent.[71] This is the equivalent increase imposed for a $5001 loss.[72]

CONCLUSION: WE SHOULD MOVE AWAY FROM SENTENCING BASED SO HEAVILY ON THE COST OF CLEANUP AND TOWARDS A SCHEME THAT DEFINES AND TARGETS INTANGIBLE HARMS

Since cost of cleanup can vastly differ for the same offense conduct, punishment levels do not reflect the seriousness of the offense.[73] Cost of cleanup does not necessarily reflect the sensitivity of the victim to intrusions, since the most loss adverse victims will probably spend less time investigating in favor of restoring service to users. Defining damage in terms of the victim's investigation and remediation costs does not promote prosecution of the more disruptive attacks. As I argue above, there are practical and doctrinal reasons that the current computer crime sentencing scheme is neither fair nor accurate. The statutory definition of loss includes investigation and remediation, but victims do not investigate or remediate in the way the law contemplates. Rather, victim choices have little to nothing to do with whether the attack was harmful or trivial.

Moreover, trivial attacks may be prosecuted more severely than destructive ones. Assume the defendant accessed a webserver through a known vulnerability and changed the webpage in Incident A. In Incident B, the defendant gained unauthorized access to a university computer and deleted all the data stored on the system. In Incident A, the webserver owner could put the system back simply by restoring the proper name to the file containing the website images. However, the owner chooses to hire expensive outside consultants to review all the computers on the system and make sure there are no other intruders or changes, taking a week's worth of work at a high hourly rate. In Incident B, the researchers restore the data from backup, taking just a couple of hours of a graduate student's time. In Incident A, the attacker could go to prison. In Incident B, despite the attacker's destructive intent and effect, the offense most likely would not be prosecuted at all.

---

[71] U.S.S.G. § 2B1.1(b)(14)(A)(i) (2005); U.S.S.G. § 2B1.1(b)(5).

[72] U.S.S.G. § 2B1.1(b)(1)(B).

[73] 18 U.S.C. § 3553(a)(2)(A) (2005).

Sentencing goals in the United States federal criminal justice system are: (1) to provide punishment levels that "reflect the seriousness of the offense;"[74] (2) to "provide ". . . fairness in meeting the purposes of sentencing;"[75] (3) to provide defendants "with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner" where rehabilitation is appropriate;[76] (4) "to afford adequate deterrence to criminal conduct;"[77] (5) "to provide just punishment;"[78] (6) to maintain "sufficient flexibility to permit individualized sentences when warranted by mitigating or aggravating factors not taken into account in the establishment of general sentencing practices;"[79] (7) "to protect the public from further crimes of the defendant;"[80] (8) "to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct;"[81] and (9) "to provide certainty . . . in meeting the purposes of sentencing."[82] Goals 1, 2, 5, 8 and 9 are not met by the current practice in computer crime sentencing.

My argument suggests several ways in which the current computer crime statute and sentencing scheme should change. Most basically, the sentencing process needs to discriminate between included and legally excluded harms. To account for investigation and to exclude reputational harm, system improvements and forensic costs, investigators and victims must be trained to maintain and provide accurate and complete documentation of post-intrusion activities. Courts should require such documentation and scrutinize it. Where

---

[74] 18 U.S.C. § 3553(a)(2)(A).

[75] 28 U.S.C. § 991(b)(1)(B) (2005).

[76] 18 U.S.C. § 3553(a)(2)(D).

[77] 18 U.S.C. § 3553(a)(2)(B).

[78] 18 U.S.C. § 3553(a)(2)(A).

[79] 28 U.S.C. § 991(b)(1)(B).

[80] 18 U.S.C. § 3553(a)(2)(C).

[81] 18 U.S.C. § 3553(a)(6); *see also* 28 U.S.C. § 991(b)(1)(B).

[82] 28 U.S.C. § 991(b)(1)(B).

courts feel a lack of competence in assessing damage estimates, experts can be useful. However, courts have no incentive to scrutinize victim loss estimates and to discriminate between proper and improper damage claims when the burden of proof at sentencing is so low.

More fundamentally, I believe sentencing computer crimes based mainly on economic loss is a mistake. These types of crimes are characterized by intangible harms which are difficult to measure economically. Fields of economics are devoted to measuring harm from security incidents, the value of privacy, and other intangibles. But these academic endeavors are too speculative, malleable, and theoretical to be the basis for prison terms.

The current Sentencing Guidelines may be moving in the right direction by identifying the type of harm that the statute seeks to prevent and by scaling the sentence accordingly. If the attack was fundamentally an invasion of privacy, courts should impose one sentence. If the attack was targeting critical infrastructure, courts should impose a higher sentence, regardless of the cost of investigation or repair. Attacks with more victims could be sentenced more severely than lesser intrusions. Attacks for the purposes of economic espionage would be sentenced more severely than website defacements. As it has begun to do, the United States Sentencing Commission could identify the harms the statute seeks to prevent and suggest adjustments accordingly.

To do this well, any sentencing authority has to consider computer crime prohibitions, the interests legislatures seek to protect through such statutes, and the relative importance of these interests to society. Ultimately, crafting appropriate sanctions for intrusions requires more understanding of and agreement about the social value of the rights and property interests commonly harmed by computer attacks. This is a worthwhile endeavor. Currently, we have Computer Fraud and Abuse Act cases, which hold that the statute prohibits issuing patently overbroad subpoenas for email[83] and for operating search engines,[84] practices that fall outside the common understanding of illegal computer hacking. Giving greater consideration to the rights and interests we are trying to protect with computer crime legislation may lead to the creation of a statute that protects us more effectively.

---

[83] Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003), *amended by and reh'g denied*, 359 F.3d 1066 (9th Cir. 2004), *cert denied*, 125 S. Ct. 48 (2004).

[84] Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).