Totem and Taboo in Cyberspace: Integrating Cyberspace into our Moral Universe[1]

Fifth edition, April 2005[2]

M. E. Kabay, PhD, CISSP[3]

1 Introduction

Cyberspace, the realm of computer networks, voice mail and long distance telephone calls, is increasingly important in our lives. Unfortunately, morally immature phreaks, cyberpunks and criminal hackers are spoiling it for everyone. Security professionals must speak out in the wider community and change the moral universe to include cyberspace.

We are seeing today a period of exploration and development in a new realm reminiscent of the colonization of North America by Europeans. As in the American experience of the frontier, there are colonists and Amerinds, soldiers and outlaws, priests and thieves. The frontier is cyberspace: that immaterial world where we have phone conversations; where credit card information travels while we wait for approval of a purchase; where our medical records and sometimes our credit records paint a picture of our pains.

For an increasing number of us, cyberspace is also the place we meet new friends and keep in touch with old ones, learn more about our hobbies and our professions, and work for social and environmental change. Electronic bulletin board systems have mushroomed throughout the world, ranging from country clubs like CompuServe and Prodigy through the grungy cafés of the hacker underground and on into the pullulating bazaar of the great Internet, where philosophers rub shoulders with dropouts and where age, gender and race are only as visible as you want them to be.

Unfortunately, the spectacular growth of cyberspace has not been accompanied by rules for civilized behavior. Cyberspace at the end of the twentieth century resembles the frontier at the beginning of the eighteenth: bullies and criminals swagger electronically through the commons, stealing what they want, breaking what they don't, and interfering with decent people's activities. Far from helping to set standards of mutual respect, some government agencies have been acting like totalitarians rather than democrats. For all these reasons, we citizens of cyberspace must evolve guidelines for civilizing our new frontier.

---

[1] Paper presented in the Panel entitled, *Interdisciplinary Perspectives on INFOSEC*. 17th National Computer Security Conference, 11-14 October 1994, Baltimore Convention Center, Baltimore, MD. Changes include corrections of errors, updates to some references and some new material.

[2] Permission is granted to copy or distribute (but not to post) this article intact as long as the copyright statement is included and the recipients are not charged for access or for copies.

[3] Associate Professor, Information Assurance / Division of Business & Management / Norwich University, Northfield, VT 05663-1035 USA

2 The Granddaddy of All Networks

The Internet is possibly the most complex and rapidly growing construct humanity has ever created. The cathedrals of medieval Europe pale in comparison with the electronic edifice that is the Internet. The Internet grew out of ARPANET, funded in the late 1960s by the Defense Advanced Research Projects Agency (DARPA). This experimental network linked a few universities and research laboratories electronically. ARPANET begat the Internet when the National Science Foundation (NSF) decided to make internetworking possible for many more universities than the first tier institutions that had been in from the beginning. ARPANET itself disappeared as a formal entity in 1990.

From the very beginning, the group inventing ARPANET had a refreshingly non bureaucratic attitude towards their work. For example, meetings of the 'Network coordinators at Bolt Beranek and Newman in 1968 had two ground rules: Anyone could say anything; and nothing was official. The current management style of the Internet reflects the belief in unhindered engineering excellence as the best way to find solid solutions for technical problems. This tradition of frank criticism and unfettered creativity has been misinterpreted by some newcomers to the Internet as an excuse for frank rudeness and unfettered criminality.

The Internet today functions like a combined mail route, supermarket bulletin board, and library. Electronic mail (e-mail) is much faster than paper mail (*snail mail* as it's derisively termed on the 'Net). Electronic Bulletin Board Systems (BBSs), Special Interest Groups (SIGs) or Forums allow us to post electronic notes asking for advice, help, friendship, and all the other dimensions of social interactions. There are electronic equivalents of newspapers (*news groups*) and magazines (*moderated news group digests*) dealing with interests from the sublime to the prurient. Scientists from distant institutions collaborate fruitfully on research without concern for geographical barriers. Textbooks and novels are posted on the 'Net (the affectionate term for the entire Internet and all the 'Networks connected to it in any way) for enjoyment and comment, sometimes coming out better for the free flow of criticism and advice. So many repositories of information are on the 'Net that doing research without using its resources is unthinkable for a growing number of enthusiasts.

Because the 'Net has grown by cooperation and consensus rather than legislation and government regulation, there is no way to know exactly how many people use how many computers on this fishnet of the mind. Generally accepted estimates are that there are about 13 million regular users linked via roughly 1.3 million computers (*hosts*). Registration of hosts has exploded since the Internet community agreed to allow commercial firms to join.

According to a document from the 'Network Information Systems Center at SRI International in Palo Alto, California, there was an 80.6% increase in the number of hosts in 1992.[4] Of the 1,313,000 hosts, 410,940 or about a third were in the educational (*.edu*) domain. Some 347,486, or about a quarter, were in the commercial (*.com*) domain. The annual growth rate in 1992 for .edu was 69%, but the growth in .com was 92%. The advent of users from .com has elicited

[4] Named, in typical style, "/infosource/internet_info_for_everybody / how big is the internet/domain survey jan93"

howls of protest from some quarters on the Internet; however, commercial users may bring new standards of behavior to the 'Net.

The total rate of information transfer in the Internet is unknown; however, it appears to be Tebibytes (TiB) per day.[5] This number, 1,125,899,906,842,624 bytes, cannot reasonably be apprehended. A byte corresponds approximately to a character of text. This article has about 50 thousand bytes (50 KiB). A 1,000 page textbook might have a few million bytes (mebibytes, or MiB) of text; that there are a million MiB in a TiB. Even more astounding, the total traffic is growing by about 25% every month – a 14-fold increase in a year.

3 A Moral Vacuum

Cyberspace is growing fast, and the values which inform our lives in physical communities have not yet found their way into cyberspace. Just as in the physical world, unethical, immoral, and illegal behavior threatens the agreements that allow people to live and work together in peace.

Many users of cyberspace are well behaved. They are sensitive to nuance, capable of expressive and articulate prose, careful not to hurt feelings, and responsible in spreading verified information and not rumor.

However, we also find the cyberspace equivalents of slum lords, drug pushers, boors and bully boys. There are people running private BBSs, Web sites, and blogs[6] that cater to thieves, drug users, Nazis, and pedophiles. People who might never think of insulting a stranger to her face write nasty and juvenile notes.

Different service providers adopt different stances about the content of communications on their network. For example, the commercial value added networks (VANs) Prodigy and CompuServe are among the most custodial in their attitude towards the message base. These services employ system operators (Sysops), volunteers who manage specific sections by monitoring traffic, responding to questions and cooling tempers. Some Sysops on commercial services and private BBSs explicitly censor unacceptable or irrelevant contributions, usually to howls of protest and hyperbolic invective from the censored authors. These howls are then themselves removed from view, prompting yet more appeals to First Amendment rights. As a Sysop myself, I have had to explain that the Forum or SIG is not public and that the Sysop has a responsibility to maintain a professional tone and to prevent abuses such as posting text files or software without permission of the copyright holders. Some moderated news groups on the Internet also have strict enforcement. For example, the RISKS Forum Digest is tightly controlled by its moderator, who personally determines whether any given message reaches the members.

At the other extreme, there are networks, Forums, SIGs, BBSs and Websites where anarchy reigns. Contributions are unfiltered, unfettered, frequently ungrammatical, and sometimes illegal. Some boards and groups pander to unusual sexual orientations, with hundreds of pornographic

[5] The prefixes kibi-, mebi-, gibi-, tebi- and so on were defined in 1998 by the International Electrotechnical Commisssion. See the Wikipedia entry at < http://en.wikipedia.org/wiki/Binary_prefix >.

[6] Weblog; see < http://en.wikipedia.org/wiki/Blog >

text and picture files available online. Others specialize in stolen or malicious software, and instructions on picking locks, stealing services and building bombs.

Such rude, unethical, immoral and illegal behavior puts the entire 'Net at risk from self appointed as well as legally delegated guardians of public morality and corporate interests. I fear that politicians looking for an easy target may impose restrictions on the content of electronic communications. Legislative interference would likely include requirements for paperwork and would render the volunteer job of Sysop impossibly demanding. The ultra religious forces of intolerance could also seize the opportunity to attack a new den of iniquity, whipping up their doctrinaire supporters to acts of harassment, sabotage and even physical violence.

4 Crimes in Cyberspace

What kinds of problems are there? The issues boil down to theft of services and software, invasion of privacy, outright damage, and the threat of terrorism.

In a landmark study, John Haugh and his colleagues at Telecommunications Advisors Inc. in Seattle, WA, have recently built up a staggering picture of the extent of toll fraud (using someone else's telephone services illegally) and telabuse (using one's employer's phone service without authorization). Haugh et al. consider that the total losses to the economy from toll fraud and abuse of corporate telephone systems are in the $2 8 billion range per year. Toll fraud rings using stolen telephone credit card numbers have been operating virtually unchecked in all major urban centers. The cycle often begins with *shoulder surfing*, in which someone watches as a victim punches their access codes into a public telephone in a public place. Organized gangs of youths have been caught in New York's Grand Central Station and La Guardia Airport. Within days, the credit card can be used for hundreds of long distance phone calls generating thousands of dollars of expense for the victim. Although the phone companies generally do not insist on repayment, these calls do cost the U.S. economy something: inter carrier charges must be paid to the national telephone services of the countries of destination. Most of the stolen calls go to South American drug havens, certain Caribbean islands, and to the Indian subcontinent.

Some criminals use control codes or special tone generators (*Blue Boxes* and others) to steal telephone services; others dial into corporate phone switches using public 800 numbers, then use outbound lines for long distance calls. Some victims have had more than a quarter million dollars of calls placed in a single weekend. The invoices from the phone companies sometimes fill several crates with thousands of call details – all fraudulent.

Voice mail subversion is another tactic used by *phone phreaks*. Voice mail systems allow callers to leave messages for specific employees. Unless supervisors pay close attention to usage statistics, a voice mail system can become host to dozens of unauthorized accounts for strangers, thus putting an unexpected load on phone lines and consuming storage space on the voice mail computers.

By far the greatest problem caused by criminal hackers is the loss of confidence in system integrity. Take for example a computer system used for production of mission critical information. There can be no tolerance for error. Programs written for such a system are subjected to strict quality assurance procedures; every program must pass extensive testing.

When the operating system (the software that coordinates communication among programs and regulates access to different kinds of computer resources) has to be changed (*updated*), many system managers run acceptance tests over an entire weekend to ensure that there will be no glitches once production starts up again. It is considered normal to forbid programmers to modify production databases; and careful audit trails are usually kept to track exactly which specific user altered what specific records at any give time in the files.

Discovering unauthorized use causes chaos in the production shop. A hospital pharmacy discovers the transposition of two digits in its pharmacy database, leading to potentially fatal errors in drug administration for patients. A faulty program in a telephone switching center disrupts phone service over an entire geographical region. Since there is no way of knowing what intruders have done (criminal hackers do not leave neat system alteration notices), the only reasonable response to intrusion is to audit the entire production system. That means time consuming, mind numbing labor to run verification programs on all the data, careful comparison of every program with a known good copy to see if it has been altered illegally, and hours of overtime for quality assurance and system management personnel.

Credit records are relatively easy for criminal hackers to find, although it's much harder to modify them. Patient files are supposed to be protected yet many hospitals have rudimentary safeguards that do not deter determined hackers. On another front, government employees have disclosed confidential information such as tax files and criminal records. In some cases the theft of data was for money (a few dollars for reports to unethical private investigators) and in others merely for fun (printing tax files of the rich and famous to impress one's friends). These are the electronic equivalent of breaking and entry in the physical world.

Another area of concern is eavesdropping. Industrial espionage is growing as competition heats up, especially across international borders. In the U.S., Symantec and Borland have been at loggerheads over the alleged theft of confidential information by an executive who defected from one company to the other. In Europe, General Motors and Volkswagen have been denouncing each other over allegations of a similar theft by a high placed official.

The last decade has witnessed a troubling proliferation of malicious software such as viruses, worms, Trojan Horses, and logic bombs. A computer virus is a program which adds itself to executable code (programs and boot sectors on diskettes and disks). When the infected code is loaded into main memory (usually on a microcomputer such as an IBM compatible PC or an Apple Macintosh), the virus can both reproduce by infecting other programs and also deliver its payload. Virus payloads range from the merely annoying (e.g., the STONED viruses usually put a plea for the legalization of marijuana on the screen) through the irritating (the Autumn viruses make the letters on one's screen drop to the bottom like so many leaves) to the destructive (viruses written by Bulgaria's Dark Avenger tend to cause random changes in data and programs anywhere on disk, leading to unpredictable and pernicious damage).

Depending on how one judges variations to be different, there are from two to four thousand recognizable viruses circulating in cyberspace. About 30 virus types account for almost all the virus infections that ordinary users are likely to encounter. STONED and JERUSALEM alone account for about five sixths of all infections. Unfortunately, criminals have put virus writing kits

into the underground networks, so now even incompetent programmers can create mutating (*polymorphic*) viruses that employ sophisticated techniques (*stealth*) to avoid detection.

Recent industry surveys suggest that the risk of virus infection of microcomputers (PCs and Macintosh) is a few percent per year per computer. There are currently no viruses found on user systems which infect large (mainframe) computers. There are only a few which affect UNIX operating systems or local area network operating systems.

The most widespread computer crime is software theft. Estimated rates of theft range from about 35 40% in the USA to 99% stolen in Thailand. Robert Holleyman, president of the Business Software Alliance, reports that more than 80% of the computer programs in China are pirated, making it one of the worst stealers of software in Asia and costing the worldwide industry US$500 million a year. Sometimes stolen programs are available in Asia before they are released legally.

Apparently China is now concerned about copyright violations in part because its own software industry is being harmed. Yang Tianxin, chief of the computer division of the ministry of electronic industry, claims that China is just beginning to attack this problem using criminal penalties and education.

Western nations also need to integrate respect for intellectual property into normal morality. Too many managers, teachers, technicians and just plain users are stealing software by making unauthorized copies of copyrighted programs. It's no wonder children trade pirated copies of computer games with no awareness of doing wrong.

Most computer crimes are not perpetrated by criminal hackers. Recent surveys suggest that about 85% of all computer related crimes are committed by personnel authorized to use the computers they abused. The probability of being attacked by outsiders is only about 1 or 2% per system per year.

Within organizations, programmers occasionally write malicious software. *Trojan Horses* are programs which have secret functions (e.g., keeping a record of passwords) along with their ostensible purposes. The AIDS Information Diskette which circulated worldwide a few years ago was a Trojan which pretended to offer information about the dread disease, but then scrambled the user's disk directory and tried to extort payment for a recovery utility. Trap Doors involve programming secret entry points for later unauthorized use; the password "Joshua" was part of a trap door left by the creator of a top secret government system in the movie *War Games.*

Logic bombs are sections of program which check for particular conditions and then wreak havoc in the system. In the film, *Single White Female*, a programmer leaves a logic bomb in her code to wipe out her creepy client's entire fashion database because he hasn't paid her full fee. In November 1993, a Manhattan programmer and his technician were accused of planting a logic bomb in a client's software when he refused to pay the full cost of the package. Some programmers insert logic bombs in their code as a matter of course.

The cyberspace equivalent of vandalism occurs when intruders or disgruntled employees deliberately damage or destroy information. The 414 Gang (so named from the area code of their

Milwaukee homes) damaged clinical research data in their forays through the 'Networks in the early 1980s. Two teenagers from Staten Island caused $2.1 million of damage to the voice mail system of a publisher by erasing orders for advertising and leaving obscene messages which offended clients. When they were finally tracked down and arrested, the 14 and 17 year-olds admitted that their depredations were revenge for having failed to receive a promised poster from the publisher.

In a report at the 16th National Computer Security Conference in Baltimore, MD in September 1993, an investigator whose team tracks the underground BBSs revealed that detailed instructions for weapons of terrorism are freely available in cyberspace. The published recipes for home made bombs were evaluated by professionals from military special forces and were pronounced to be workable, albeit dangerous for amateurs.

Some administrators at universities with Internet connections have been put under opposing pressures because of the availability of graphic pornography graphics. There have been threats of lawsuits for allowing such materials to enter the campus systems and threats of lawsuits for forbidding such materials to enter the campus systems. Some pedophile BBS operators have been found to use their systems to entice youngsters into meetings by offering illicit files and cheap stolen hardware and software. It is easy to create false identities through electronic mail. Some denizens of cyberspace use one or more pseudonyms (*handles*). A major hacker conference was announced on the Internet by *drunkfux@cypher.com* with no other identification made available. Some *cypherpunks* insist that there should be no interference with this practice, arguing that any attempt to enforce identification would be a gross infringement of their privacy.

Advocates of anonymous and pseudonymous postings defend their preference by pointing to the long standing acceptance of pseudonyms in print. I wonder if they would defend wearing face masks during face-to-face conversations?

5 Who Are the Technopaths?

Because of the shadowy nature of the computer underground, where real names are few and role playing is the norm, it is hard to find reliable statistics about the demographics of what famed Bulgarian anti virus researcher Vesselin Bontchev (later at the University of Hamburg) has called *technopaths*. The consensus in the computer underground is that they are predominantly teenaged boys and young men. These maladapted, undersocialized, emotionally underdeveloped individuals adopt handles such as *Phiber Optik, Acid Phreak, Dark Avenger, The Leftist, The Prophet, The Urvile,* and *Necron 99*. They form electronic gangs with ludicrous names like *Masters of Deception* and *Legion of Doom*. Much of this is adolescent posturing; as one member of the latter group commented, "We couldn't very well call ourselves the Legion of Flower Pickers."

Several popular books have provided insights into the psychology of criminal hackers. One of the best is by Katie Hafner and John Markoff.[7]

[7] *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone Books, Simon & Schuster (New York, 1991). ISBN 0 671 77879 X. 368 pp. Index.

Sarah Gordon of the IBM T. J. Watson Research Center has written extensively on her interviews with virus writers.[8] Her main point is that the virus-writing community (and probably the criminal hacker community) should not be viewed as monolithic, but rather that it is composed of a wide variety of personality types and stages of moral development.

6 Are Some Hackers Crazy?

The standard reference work on psychiatric disorders[9] defines the Narcissistic Personality Disorder in these terms:

A pervasive pattern of grandiosity (in fantasy or behavior), need for admiration, and lack of empathy, beginning by early adulthood and present in a variety of contexts, as indicated by five (or more) of the following:

- *Has a grandiose sense of self-importance (e.g., exaggerates achievements and talents, expects to be recognized as superior without commensurate achievements).*
- *Is preoccupied with fantasies of unlimited success, power, brilliance, beauty, or ideal love.*
- *Believes that he or she is "special" and unique and can only be understood by, or should associate with, other special or high-status people (or institutions).*
- *Requires excessive admiration.*
- *Has a sense of entitlement, i.e., unreasonable expectations of especially favorable treatment or automatic compliance with his or her expectations.*
- *Is interpersonally exploitative, i.e., takes advantage of others to achieve his or her own ends.*
- *Lacks empathy: is unwilling to recognize or identify with the feelings and needs of others.*
- *Is often envious of others or believes that others are envious of him or her.*
- *Shows arrogant, haughty behaviors or attitudes.*

Associated Features:

- *Depressed Mood*

[8] Gordon, S. (1994). The generic virus writer. < http://www.research.ibm.com/antivirus/SciPapers/Gordon/GenericVirusWriter.html >;
– – - (1994). The generic virus writer II. < http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html >;
– – -(1993). Inside the mind of Dark Avenger. < http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html >

[9] American Psychiatric Association *Diagnostic and Statistical Manual IV.* < http://www.psychologynet.org/dsm.html >

- *Dramatic or Erratic or Antisocial Personality*

Differential Diagnosis

Some disorders have similar or even the same symptom. The clinician, therefore, in his diagnostic attempt has to differentiate against the following disorders which he needs to rule out to establish a precise diagnosis.

- *Histrionic Personality Disorder*
- *Antisocial Personality Disorder*
- *Borderline Personality Disorder*
- *Obsessive-Compulsive Personality Disorder*
- *Schizotypal Personality Disorder*
- *Paranoid Personality Disorder*
- *Manic Episodes*
- *Hypomanic Episodes*
- *Personality Change Due to a General Medical Condition;*
- *Symptoms that may develop in association with chronic substance use.*

Cause:

The cause of Narcissistic Personality Disorder is unknown at this time, but several theories are being investigated. There is some evidence that genetic predisposition and other biological or biochemical factors are involved for some people. Psychological factors are also involved for most people.

Treatment:

Treatment of Narcissistic Personality Disorder usually consists of individual, group or family therapy, structure (scheduling one's time so that there are no long periods of unplanned time), support, medications, limit-setting, consistent rules, education about the illness, social skills training, behavior modification and learning more effective communication and coping skills. Inpatient or day hospitalization may be necessary when symptoms make the patient a danger to self or others.

Sound like some hackers you've read about or even met?

During the 1990 December holiday season, some 250 hackers gathered for their Christmas Con in a hotel near Houston airport. After consuming too many beers and pulling fire alarms, the group was evicted from the hotel. This sort of behavior is associated with the Antisocial Personality Disorder, described as follows:

There is a pervasive pattern of disregard for and violation of the rights of others occurring since age 18 years, as indicated by three (or more) of the following:

- *Failure to conform to social norms with respect to lawful behaviors as indicated by repeatedly performing acts that are grounds for arrest.*
- *Deceitfulness, as indicated by repeated lying, use of aliases, or conning others for personal profit or pleasure.*
- *Impulsivity or failure to plan ahead.*
- *Irritability and aggressiveness, as indicated by repeated physical fights or assaults.*
- *Reckless disregard for safety of self or others.*
- *Consistent irresponsibility, as indicated by repeated failure to sustain consistent work behavior or honor financial obligations.*
- *Lack of remorse, as indicated by being indifferent to or rationalizing having hurt, mistreated, or stolen from another.*

The individual is at least 18 years old (under 18 see Conduct Disorder). There is evidence of Conduct Disorder with onset before age 15 years and the occurrence of antisocial behavior is not exclusively during the course of Schizophrenia or a Manic Episode.

Associated Features:

- *Depressed Mood.*
- *Addiction.*
- *Dramatic or Erratic or Antisocial Personality.*

Differential Diagnosis:

Some disorders have similar symptoms. The clinician, therefore, in his diagnostic attempt has to differentiate against the following disorders which need to be ruled out to establish a precise diagnosis.

Substance-Related Disorder;

- *Schizophrenia*

- *Manic Episode*
- *Narcissistic Personality Disorder*
- *Histrionic Personality Disorder*
- *Borderline Personality Disorders*
- *Paranoid Personality Disorder*
- *Adult Antisocial Behavior.*

Cause:

The cause of this disorder is unknown, but biological or genetic factors may play a role. The incidence of antisocial personality is higher in people who have an antisocial biological parents. Although the diagnosis is limited to those over 18 years of age, there is usually a history of similar behaviors before age 15, such as repetitive lying, truancy, delinquency, and substance abuse. This disorder tends to occur more often in men and in people whose predominant role model had antisocial features.

Twin studies have confirmed the hereditability of antisocial behaviour in adults and shown that genetic factors are more important in adults than in antisocial children or adolescents where shared environmental factors are more important. . . .

Cadoret et al (1995) studied the family environment as well as the parentage of adoptees separated at birth from parents. Antisocial Personality Disorder in the biological parents predicted antisocial disorder in the adopted away children. However, adverse factors in the adoptive environment (for example, "marital problems or substance abuse) independently predicted adult antisocial behaviours.[10]

In 1993, some of the 200 attendees at HoHoCon in Austin pulled fire alarms after a night of drunken carousing and viewing pornographic movies. In the Austin HoHoCon in December 1993, criminal hackers discussed cracking cellular phones, shared information on new techniques for stealing long distance services, and boasted of posting anarchist files on BBSs. When I challenged a criminal hacker calling himself after a vegetable for having posted instructions on how to make bombs out of household cleaning supplies, his friends glared angrily at me and hissed, “It wasn’t illegal. He had a right to post whatever he wanted.” The hacker rejected responsibility for the consequences of his actions; although he regretted that two children had recently destroyed their hands in an explosion while following the details of his file, he sneered that perhaps it was evolution in action. He admitted that maybe it seemed wrong, but he didn’t know why. “And anyway,” he shrugged, “who’s to say if it’s right or wrong?” “Who’s to say??” I asked. “*You* are. *I* am. *We* are!”

[10] See < http://www.psychnet-uk.com/clinical_psychology/criteria_personality_antisocial.htm >

The culture of criminal hackers seems to glorify behavior which would normally be classified as sociopathic or frankly psychotic. These behaviors must not become normative.

7 Technical Solutions

Technical approaches to behavioral problems have a limited scope. Some attempts to protect cyberspace concentrate on making it harder to do harm. For example, system managers are supposed to pay strict attention to how people can enter their systems and networks; this area of concern is known as access control. Some of the more successful methods currently in use include one time password generators. Such hand-held units, about the size of a credit card, generate random looking codes which can be used for logging into computer systems and networks, but which are valid for only one minute.

Modems which garble transmissions make it impossible to crack systems using brute force methods. Instead of trying hundreds of passwords without hindrance, criminal hackers would be forced to turn to the much slower techniques of lying and spying (social engineering). Even if criminal hackers were to enter a secure system, encrypted data would severely interfere with their ability to cause trouble. Unfortunately, encryption is still not in general use in the business community.

Finally, if more victims of computer crime were to report what happened, the computer security industry could develop the same kind of shared expertise as the insurance industry's actuaries. It would help immeasurably to have a library of documented case studies of computer crime available for study by computer science students, sociologists, criminologists and security experts. All organizations hit by computer criminals are encouraged to report what happened to the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University in Pittsburgh, PA.[11]

8 Human Solutions

Technical solutions appeal to the rational propensities of security specialists. But since people are at the core of computer crime, psychosocial factors must be at the core of efforts to contain it.

Security is the tooth flossing of the computer world: it's boring and repetitive, slightly distasteful, and has no obvious, immediate benefits. Even worse, the better the implementation, the less frequently problems arise. Ironically, the very success of security measures may reduce the credibility of the security team in the eyes of amateurs.

In any case, security cannot be achieved by superficial changes of style. Just as the Total Quality Management movement emphasizes that the concern for quality must pervade all aspects of working culture, information security must become part of the corporate culture.[12]

[11] http://www.cert.org

[12] See the Wikipedia entry on TQM at < http://en.wikipedia.org/wiki/Total_Quality_Management >

Security professionals have to deal with the psychological difficulties of trying to change deeply rooted patterns of social behavior. For example, a typical security policy states that no one may allow another employee to "piggyback" into a secure area; that is, each person entering through a secured door must use their own access control device. However, politeness dictates the opposite: we hold a door open and invite our friends and colleagues to enter before we do. To learn new habits, it is useful to address the conflict directly: acknowledging that the policy will be uncomfortable at first is a good step to making it less uncomfortable. For example, employees should participate in role-playing exercises. First, they can practice refusing access to colleagues who accept the policies graciously, then move on to arguments with less friendly colleagues. Finally they can learn to deal with confrontations with colleagues who pretend to be higher rank and hostile. Managers should practise being refused access to secured areas.

In grade schools, high schools, colleges and universities, students are introduced early to computer systems and expected to master and use computers in their studies. All too often, however, ethical issues about computer usage are neglected. Some instructors blatantly steal copyrighted software or tell their young charges to do so ("Here, copy this diskette and return the original"). Other children entrain their younger contemporaries into the glitzy world of computer virus exchanges and virus writing. There's always the allure of computerized pornography on the Web – an allure enhanced by the lack of knowledge of parents and teachers about the very existence of such sources.[13]

Lonnie Moore is computer security manager at the Lawrence Livermore National Laboratory. With the help of Gale Warshawsky, an employee who happens to be an experienced puppeteer, Moore has created an appealing and entertaining security awareness video for children in elementary schools. The heroes are Chip, the friendly computer, and Gooseberry, the hapless untrained user. The villain is Dirty Dan, the nasty hacker. Dan drops crumbs into Chip's keyboard, destroys files and makes Chip cry, then makes Chip dizzy by feeding him a virus from another computer. Moore explains, "What we're trying to do is learn from the mistakes that have been made. They understand good guys and bad guys. We also teach them to try to have some feeling for the others involved."

A major telephone company in the U.S. has created a video for middle school children which addresses telephone fraud in an entertaining and informative way.

9 Ten Cyber-Commandments

The Computer Ethics Institute in Washington, DC, has published the Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.

2. Thou shalt not interfere with other people's computer work.

3. Thou shalt not snoop around in other people's computer files.

[13] See Kabay, M. E. (2002). *Cyber-Safety for Everyone: from Kids to Elders.* < http://www2.norwich.edu/mkabay/cyberwatch/index.htm >

4. Thou shalt not use a computer to steal.

5. Thou shalt not use a computer to bear false witness.

6. Thou shalt not copy or use proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.

8. Thou shalt not use other people's intellectual output [without due acknowledgement].

9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.

10. Thou shalt always use a computer in ways that demonstrate consideration and respect for your fellow humans.[14]

Efforts such as these are the beginning of a response to lawlessness in cyberspace. Operating at the human level, they are ultimately as important as technical solutions to computer crime.

10 The Moral Universe of Computer Users

It takes time to integrate morality into our technological universe. Twenty years ago, many drivers felt that driving under the influence of alcohol was adventurous. Today most people feel that it's stupid and irresponsible. Smoking in public is becoming rare. Many of us in northern cities have witnessed exiled smokers huddled together in the cold outside buildings where they once lit up with impunity.

Similarly, we need a consensus on good behavior in cyberspace.

Criminal hackers who break into computer systems and roam through users' private files should be viewed as Peeping Toms. Criminals using computers to extort money or steal services should be recognized as thieves. Those who destroy records, leave logic bombs, and write viruses should be viewed as vandals. Hackers who smear obscenities in source code should be seen as twisted personalities in need of punishment and therapy. Government agencies proposing to interfere in electronic communications should be subject to scrutiny and intense lobbying.

Beyond such prohibitions and inhibitions of taboos, cyberspace needs the electronic equivalent of Emily Post. We need to discuss the immorality of virus writing, the ethical implications of logic bombs, and the criminality of electronic trespassing. We should teach children how to be good citizens of cyberspace – and not just in schools. We should sit down with computer using youngsters and follow them through their adventures in cyberspace. Parents should ask their teenaged whiz kids about hacking, viruses, software theft and telephone fraud. We must bring

[14] Computer Ethics Institute. < http://www.brook.edu/its/cei/overview/Ten_Commanments_of_Computer_Ethics.htm >

the perspective and guidance of adult generations to bear on a world that is evolving faster than most of us can imagine.

Participants in the National Computer Security Conferences [later the National Information Systems Security Conferences which terminated in 2000] should be at the forefront of efforts to reach out into the wider community. If experts in security cannot express their values, who will?

The adolescent confraternity of criminal hackers and virus writers have already begun developing totems: the personae of Dark Avenger and Acid Phreak loom over youngsters much as Robin Hood once did for another generation.

What we need now are taboos to match the totems.

You are welcome to write to me with comments and questions:

M. E. Kabay, PhD, CISSP
< mailto:mkabay@norwich.edu >
Division of Business and Management
Norwich University
158 Harmon Drive
Northfield, VT 05663-1035

