Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Ethics in the IT Community

This paper is an overview of the current state of ethics in the IT community. It describes the current state of ethics in IT, identifies the major areas of concern for the IT community, and discusses the relationships an IT professional will face, and the conflicts that may jeopardize those relationships. Central to this paper are the ideas that as a professional in the IT community, we must act in an ethical manner if we wish to keep the trust of our customers, be they our employer, our client, or the public at large....

Copyright SANS Institute
Author Retains Full Rights

AD

Ethics in the IT Community

Anthony D. Bundschuh
November 1, 2004
GSEC Practical Assignment Version 1.4c
Option 1 - Research on Topics in Information Security

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

ABSTRACT

This paper is an overview of the current state of ethics in the IT community. It describes the current state of ethics in IT, identifies the major areas of concern for the IT community, and discusses the relationships an IT professional will face, and the conflicts that may jeopardize those relationships. Central to this paper are the ideas that as a professional in the IT community, we must act in an ethical manner if we wish to keep the trust of our customers, be they our employer, our client, or the public at large.

Many examples are used to illustrate the behavior, both ethical and unethical, of IT practitioners, including professionals, the general user, and those wishing to commit crimes using computers. The examples show how acts many view as innocent can be unethical and should be avoided. The intent is to convince that every aspect of IT must be looked at in a broader sense to avoid ethical issues and their consequences.

© SANS Institute 2005, Author retains full rights.

INTRODUCTION

Ethics have been the norm in the business world for many years. Ethical behavior is expected of professionals in almost all industries. Even though the Information Technology (IT) community is much different than many other industries, and some concerns may be exclusive to the profession, the same ethical standards can apply to all industries.

When a person's life is affected by some aspect of information technology, one needs to ask: Did the administrators or developers feel the need to follow an ethical code of conduct? Did a code of conduct even exist? These are the questions facing the IT community today. However, the information technology industry has been slow to catch on, with laws governing the ethical behavior of IT professionals leaving much to be desired. Many professionals argue that the state of ethics in the IT arena needs to improve.

STATE OF ETHICS IN THE IT COMMUNITY

What are ethics, and why are ethics necessary in the world today? Also, who is responsible for ensuring their compliance? Potter Stewart, Supreme Court Justice from 1958-1981, once said that ethics are "knowing the difference between what you have the right to do and what is the right thing to do." (Davis) Primarily, ethics are the codes of conduct that management and professional organizations institute, and professionals in all occupations follow, to ensure that they protect the privacy and earn the trust of the customers. These codes cover many aspects of behavior, such as the appropriate use of company IT equipment. Laws are also in place in many industries to legislate the ethical behavior of professionals. An example is the well known "doctor/patient confidentiality" standard which protects the privacy of medical information.

Some experts have a different view of ethics. One view is that ethical behavior cannot be coerced or mandated. M. van Swaay believes

> because ethical behavior implies free choice, it cannot be captured in rule. The standard of reference for what is ethical has to exist 'outside human definition', and therefore cannot be open to human negotiation.

This places the burden squarely on the individual and not on the industry, management, or the government. Because it cannot be "captured in rule" it has to come from an individuals desire to do the right thing. An individual must have an understanding of what is expected in all aspects of duty and responsibility. Knowing what is expected, the choice can be made to adhere to the standards, or to ignore them and act in an un-ethical way. However, this does not completely remove all responsibility from others, since even though the ethical behavior must come from within, as IT professionals we should lead others by our examples of ethical behavior, and let it be known that any other actions will not be accepted.

© SANS Institute 2005 Author retains full rights.

The individual may bear the burden for ethical behavior, but rarely in the IT world does the individual face the consequences. As an individual, IT professionals are usually considered just a member of a team. Also, IT is not often seen as the provider of the product or service. IT is usually looked at as the provider of tools to meet the goals of the business, not the business itself. Further, "IT practitioners rarely work in a stand-alone manner…and therefore their individual responsibility from an ethical perspective is very much diluted." (Andronache) This is a serious shortcoming of the IT community. Without fear of consequences, not much strength can be put behind the expectation of ethical behavior. It allows the un-ethical professional to take the attitude that no one can enforce the standards, therefore they do not exist. With this lack of real enforcement, those responsible for implementing and enforcing ethical standards are left without the tools to fulfill their responsibilities.

The IT industry has reached a point where it is totally pervasive in our everyday lives. Almost everything we do, everyday, is influenced or controlled by an IT system. In fact, "in western societies more people are employed collecting, handling and distributing information than in any other occupation." (Mason 5) This is mainly because of the IT industry's presence in most other industries. Without IT, these businesses would not be able to continue to operate at the staggering pace that has developed following information technology's acceptance into the realm of real business. Therefore, if ethics is necessary in the banking industry, or the medical industry, then there is a need for them in IT, especially since IT exists in all of these other industries. (Andronache) But when the number of professionals employed in the IT arena is taken into account, not to mention the vast amount of personal data and other information it controls, it shows that the need for a comprehensive ethical standard for IT is just as important, else the consequences can dire.

Richard De George sees this attitude as a sign that most corporations have not made a conscious effort to take their businesses into the information age. In his talk to the Center for Business Ethics, Bentley College, he introduces what he calls the "Myth of Amoral Computing and Information Technology." He describes it as a "failure both to accept and to assign responsibility" for failures of systems. If something goes wrong, those that do not understand the technology feel they are in no place to blame someone for the failure. (De George) This is a disturbing trend among those that provide these tools. In America, if a car is found to be unsafe, the manufacturer is held responsible. Conversely, if a new information technology has a vulnerability that can cause harm, either physically or financially, the same consumers are slow to attack the manufacturer. In fact, we continue to buy faulty products, only to complain among ourselves about the poor quality of the product. We even spend more money to make the product more secure by buying additional products to correct flaws inherent in the original product. It appears that the "myth" prevents us from seeing the truth that the producers should be expected to improve their product, or at least help the users to ensure that the issues are corrected. Microsoft and other software companies do attempt to provide this service to their users as evidenced by the Windows Update feature available on the Internet.

© SANS Institute 2005 Author retains full rights.

So we have the perspective of individual responsibility, but the individual faces no real consequences for unethical behavior. We have attempts by management and the government to mandate ethical behavior, but the disregard by both of the standards they have instituted. The worker is told to act in accordance with the standards, and report violations, but then is told to keep silent or face reprisals. We have inferior products, but only minimal efforts on the part of the producers to improve them. The challenge facing the IT industry is to change the reality of the industry and improve the ethical standards.

For an example of how poorly the IT community handles responsibility, one only needs to look at the Y2K scare that resulted in a stockpiling of weapons and toilet paper before the turn of the millennium. An understanding of the true nature of the Y2K problem shows the lack of ethical behavior on the part of the software developers and business managers alike. The extent of the issue was "hid comfortably under the shield of a technical problem." (Andronache) The developers failed to use the technology present at the time to its potential by only using two digits for the year in dates instead of four digits. It was known even then that this could be a problem, but it was ignored. The thought was that the software developed at that time would no longer be in use when the year 2000 rolled around. Even though this was not the case, that many of the programs were still in use in critical systems, no one felt that the blame lied upon the developers. (Andronache)

The developers were not the only ones who may have acted unethically. Many managers also added to the problem. They refused to pay attention to the claims of the IT personnel. They showed a lack of concern by their procrastination in dealing with the issues presented to them. Although it is felt that many did not understand the scope of the issue, those that did refused to spend any money to fix the problem. This refusal resulted in an increased cost of the solutions, a cost that must have been passed on to consumers and share holders.

As far as the public was concerned, many felt the whole frenzy was purposefully exaggerated in an effort to exploit the frenzy for personal gain. After the passage of January 1st, when none of the predictions came true, the ethical questions were raised, but not much attention was given to them. This is an example of the power that the lack of knowledge can give to those in a position to exploit it.

The Y2K scare is a good example of the impact that the unethical performance of one's job duties can affect the security of an IT system. If this had been a system vulnerability instead, the failure to fix the known problem could have had much different consequences. As will be discussed further with malicious code, a known vulnerability can have a devastating impact when used to attack a system that could be running on millions of computers.

ETHICAL AREAS OF CONCERN

So we have established that there is a need for ethics in the IT industry. Yet, the IT community has neglected to address these ethical issues. Tatiana

© SANS Institute 2005 Author retains full rights.

Andronache states in her article Hide and Seek: The Question of Ethics in IT – Part 1, "events such as Y2K, the dotcom crash, and the recent string of corporate accounting scandals, have pushed the question of ethics in IT into the spotlight." De George stated "the move of business to the information age raises many ethical issues, but has received little ethical attention." However, some ethical professionals have identified concerns and addressed many solutions, from codes of conduct to legislation. Richard O. Mason identifies in Four Ethical Issues of the Information Age the four major areas of concern: privacy, accuracy, property, and access. These concerns are vital to the protection of the customer, or user, and the proper functioning of the systems themselves.

Privacy

The drive for information privacy is epidemic in America. It is obvious that if the data is not protected properly, sensitive personal information could find its way into the hands of less than honest individuals that may injure the customer. It is even possible that the competition could get proprietary information, negating the competitive edge such information could provide. (Mason) What is not so obvious is the way in which the government or corporations can use personal information to their benefit, and possibly your harm.

Information privacy is perhaps the oldest ethical concern associated with IT. In the 1960's and 70's, privacy concerns over the government's use of vast databases of personal information about its citizens led to claims that the U.S. Congress was trying to create a "big-brother government." (Bynum) Why this concern exists, and why it is even more important today, is the "ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information." (Bynum) Databases can be assembled from smaller databases to create huge stores of information. The uses of this information can range from marketing specific products on a more personal level, to the identification and capture of criminals, all the way to the oppression of certain segments of the population. (Mason) It is clear that the uses can be beneficial, but it is also possible that the assemblage of many threads of data into one comprehensive record can invade our right to privacy in a way which was not possible before.

It should be clear how important an individual's privacy can be. What is so surprising is the freeness that many people have with their "private" information. One only has to look at the example set by the company Free-PC.com. The concept was to give a free PC (actually a two year lease) to specifically chosen applicants. The applicants only had to provide personal information, agree to use the PC for a minimum of 10 hours per month, and be bombarded by "one-to-one targeted marketing" ads at all times. (Free-PC.com) The initial offer was for 10,000 PC's, but Free-PC.com was overwhelmed by the 500,000 responses they received.

The response to the campaign shows that many people are willing to give away the personal information in many ways, sometimes for little or no compensation. All the while, many are complaining that not enough is being

© SANS Institute 2005 Author retains full rights.

done to protect their privacy. There are many advocates for information privacy, but the conflict lies in how to protect something that many value so little they are willing to give it away. (De George)

Going hand in hand with privacy is the concept of anonymity. If one can browse the internet freely without identity, then effectively privacy is protected. This can be a useful tool when accessing resources that when associated with an identity can adversely affect a person's mental or physical well being, such as medical resources that could lead to a conclusion about one's health. Of course, this concept of anonymity can also protect those looking to cause harm. A person trying to distribute child porn or lure young children away from safety can hide behind this anonymity and be unreachable by authorities. (Bynum)

Accuracy

The very nature of the IT industry is the collection and analysis of data. It stands to reason that if the data is not accurate it can seriously affect this process. Inaccurate data will result in worthless decisions based upon the data. This could result in lost revenue, or even legal ramifications. (Mason) The effects of inaccurate information can be insignificant, such as a store running out of an item because their inventory was incorrect. This may affect those that travel to the store to buy the item, but the overall impact is small.

Effects of disinformation can also be serious, from personal misfortune to societal woes. The wrong information can cause effects ranging from personal financial issues all the way to political and government control of a society. As De George states, "together with [data] ownership goes power, and with it the dangers of control and manipulation." For data owners, this is similar to the product liability faced by manufacturers for many years now.

But there are two major hindrances to information accuracy. The first is the amount of information dealt with on a daily basis. Mason claims "today we are producing so much information about so many people and their activities that our exposure to problems of inaccuracy is enormous." De George concurs believing we have now reached the point of "information overload." The difficult task lies in sifting through all of the bad information to get to the good. The amount of bad information has grown to the point that it can completely overshadow useful information. For proof, just consider the many number of search engines on the Internet. This information overload has resulted in a great economic opportunity for companies like Yahoo and Google.

The second barrier to accuracy is the community of the Internet itself. The Internet is what it is because it allows access to everyone. Not only can you find anything you can think of, but somewhere, someone is providing anything you can think of. The issue is that there is no control, no peer review, and no obstacle to keep the accurate information from being overshadowed by the disinformation. How do you know if you are looking at the information published by an authority, or a crackpot? In short, you don't. Also, the posters of the inaccurate information are not held liable for their lack of ethics. The means to prevent the mass posting of disinformation are non-existent. (De George) The

© SANS Institute 2005 Author retains full rights.

ethical issue is the providing of information that someone believes is correct even if they are not qualified to present it. Vast numbers of people are providing information that is misleading, influencing people to take actions that may cause them harm. They provide medical, financial, and legal advice without the training or education to do so. Even if controls existed, the sheer number of websites would prevent the enforcement of these controls. Hear is where individual responsibility should take over. A sense of right and wrong may stop some, but without consequences, many are still acting un-ethically.

So, it is clear that the Internet does both a service and a disservice at the same time. As users we must use all the common sense we can muster to make our way through the bad information to find the good.

Property

The area of property is concerned with the rights to use or share the data in question. Is it ethical to freely use or share information that belongs to another, even if this use could deprive the owner of the income generated by said ownership? There are two major ways that the non-ethical use of data affects the data owners; piracy and plagiarism.

The issue of software pirating has made its way to the forefront with a bang. Few have not heard of Napster and the lawsuits that ensued following it widespread use to share files. Next up was KaZaa, and the over 800 subpoenas issued to the file sharing software's users when the Recording Industry Association of America (RIAA) began its campaign to end the sharing of pirated MP3's. (USA Today) The RIAA and even the Motion Picture Association of America (MPAA) are fighting back against piracy with these lawsuits. They are not the only industries affected. The Software & Information Industry Association estimates that the software industry loses between $11 billion and $12 billion annually. (SIIA)

Even though there are countermeasures in place in the form of copyrights and patents, the digital age makes this abuse extremely easy. It is expensive for a company to develop software, or for a record company to record and issue a CD. But, with the use of file sharing programs, CD-R's, the misuse of shareware, the misuse of personal software for business use, among others, many users engage in piracy. Many may not even understand they are doing it. (SIIA)

Opponents of software licensing believe "that all information should be free, and all programs should be available for copying, studying and modifying by anyone who wishes to do so." (Bynum) This idea is not shared by the producers, for if it was, they would not take on the considerable expense to produce it they would not be able to get a return on their investment. (Bynum) Even so, it is hard for the average user at home to shell out another $200 for an additional copy of Microsoft Windows simply because he has two computers. Although the SIIA agrees that piracy will not end in the near future, the combination of "continuing education and enforcement efforts" are responsible for a drop in software piracy of nearly 50% between 1989 and 2002. (SIIA)

© SANS Institute 2005 Author retains full rights.

Unlike piracy, plagiarism was not created by technology and the internet. As anyone who was a student before the late 1980's can attest many people have copied, and passed off as their own, the work of another. No, in fact plagiarism has been around for a long time. But technology and the internet have made it so easy that a Center for Academic Integrity survey resulted in nearly 80% of college students admitting to cheating at least one time in their college careers. (CAI)

One search on the internet will reveal many websites willing to sell research papers to any student with a credit card. One website, Research Papers Online (http://www.ezwrite.com/) lets you search their "2 Research Paper Databases with more than 60,000 new Research Papers!" Search for the paper you want, pay the fee, and you are the proud owner of a high quality research paper. Plagiarism.org (http://www.plagiarism.org/) describes why the trend has increased so. They believe that in times before the wide availability of electronic resources, the task of finding the work and copying to your paper was almost as time consuming as writing the paper yourself. That is no longer the case. With cut and paste, you can assemble a paper in no time. Add to that the almost limitless sources available, and plagiarism is easy to do, and difficult to prove. (Plagiarism.org)

This position does account for the increasing ease of cheating, but it does not account for the increasing lack of ethics in the students. Why is it that so many students find it acceptable, if not normal, to cheat in this way? John Barrie, the creator of anti-plagiarism software and founder of Turnitin.com, has an idea why this is. He says the Internet is "a 1.5 billion-page searchable, cut-and-pasteable encyclopedia" for the student that is desperate for good grades. (Bartlett) He blames the plethora of information available on the Internet, the difficulty of proving plagiarism, and the competitiveness of the academic culture for the increasing rise in cheating. Many students feel that if you need to cheat to get into the desirable schools, then, cheat you must. (Bartlett)

As De George claims, the rise of plagiarism, along with the rise in pirating, is symptomatic of the decrease in ethics. It is the one ethical ideal that seems to be the easiest to abandon. Is it the lack of responsibility many younger people possess, or merely a side-effect of technology? Plagiarism.org states that many people would not consider stealing something tangible, like the words in a book or even the book itself. However, to them stealing ideas and words from the Internet is not perceived as stealing. This attitude is shared with the many people that feel software pirating is acceptable.

Access

Access does not seem at first glance to be an ethical issue. If someone is either economically poor enough that he or she cannot purchase a computer, what ethical responsibility do we have to change these conditions? Similarly, if a person lives in a country where the infrastructure does not provide access to the Internet, does that mean that we are acting without ethics if the necessary steps to provide access are not taken? Mason believes that this is so. Although

© SANS Institute 2005 Author retains full rights.

computers and other technologies have become cheaper, they are still out of reach of many in the poorer classes of society. Additionally, many of the resources once available for free from your public or school library are no longer available, because the cost to access the replacement resources are prohibitive for the facilities that once provided the service.

Terrell Bynum takes the information gap a step further. He suggests that if steps were taken to ensure information access to everyone, it would have a significant impact on many aspects of the lives of those that currently have no access. Perhaps this access could educate the uneducated, or even provide a sense of community and belonging to those in the underprivileged world.

It is believed that this information gap is widening. That many people are being left behind, and are becoming increasingly unable to contribute to society as a result. Mason feels that "we are creating a large group of information poor people who have no direct access to the more efficient computational technology and who have little training in its use." He implies that things are only getting worse. However, the American Library Association (ALA) urges libraries to take steps to ensure that they continue to provide the informational service they always have. They take the ethical stand that "libraries that raise barriers to access damage their credibility with their users." They state that it is the responsibility of the library to grant access to "information across the spectrum of human interests…even those that some people may consider false, offensive, or dangerous." It is a different view than most would think, but it still falls under the realm of ethics.

OTHER ETHICAL CONCERNS

Computer Crime

Computer crime is one aspect of computer ethics that I feel does not fit into the concepts discussed earlier. For one thing, most of the concepts of ethics deal with good intentions that sometimes go bad. Most IT professionals intend to do the right thing, but ethical actions can be difficult to understand. In the case of computer crime, the perpetrators have no good intentions. Their only intentions are to cause harm. They break into systems, plant malicious code, or steal information or money. There is nothing ethical about that, and no system of ethics can prevent intentional wrong doings.

Computer crime comes in many forms, but the most prevalent are malicious code, hacking or breaking into a system, and other computer crimes such as embezzlement. All of these crimes can be committed by insiders, or outsiders. Many IT professionals attempt to protect their systems from crimes, using tools such as firewalls, enforcing password integrity to prevent unauthorized use, and installing anti-virus programs to prevent malicious code. These measures are fairly effective, but not complete. In fact, computer crime costs the American economy over $500,000,000 each year. (Standler) Ronald Standler has this to say about computer crime:

© SANS Institute 2005 Author retains full rights.

> Experts in computer security, who are *not* attorneys, speak of "information warfare". While such "information warfare" is just another name for computer crime, the word "warfare" does fairly denote the amount of damage inflicted on society.

This paints a fairly grim picture on the state of information security in today's world.

The major obstacle to computer crime is unseen attacks. A good hacker can cover his tracks, and programmers that write code to embezzle money or cause damage are very proficient at making the process run undetected. Some crimes are perpetrated by trusted employees making it hard to defend against by increasing the defenses against internet attacks. (Bynum) These factors are becoming increasingly difficult, as seen by the increase in programs such as Sans' Information Security certifications to attempt to prepare professionals to battle these crimes.

Another factor that hinders effective information security is the rate at which vulnerabilities are discovered in software. The statistics in the following table were reported by CERT.org, and show the rapid increase in the number of software vulnerabilities that are reported each year. The rate at which vulnerabilities are discovered seriously hinders the ability of system administrators and Information Security to protect their systems.

Vulnerabilities reported

Year	1995	1996	1997	1998	1999	2000	2001	2002	2003	1Q-2Q 2004
Vulnerabilities	171	345	311	262	417	1,090	2,437	4,129	3,784	1,740

While it is possible that many of these vulnerabilities are discovered by professionals that are trying to improve the state of information security, many must be found by those wishing to find ways to harm systems or steal information. As such, they may be posted on hacker websites long before a patch is released to correct the vulnerability. This delay in the release of patches provides a window of opportunity for the hacker in which to exploit the vulnerability without hindrance. Couple that with the sheer number of vulnerabilities and it is virtually impossible to ensure that all of the software employed on a system is properly patched and protected.

The IT Professional

This brings us to the most important part of this paper, the responsibilities we all face as IT Professionals. There are many organizations out there that have some sort of code of conduct for the members of its community to follow, and IT is no different. The website Codes of Conduct/Practice/Ethics from Around the World lists many professional organizations that provide codes. It is evident that there are many that wish to improve the state of ethics for the IT

© SANS Institute 2005 Author retains full rights.

community, and any of these codes would be a good starting point for a professional or organization to shape ethical behavior.

The established codes fulfill a service by defining a standard of behavior, but they may not be sufficient in setting standards for every situation that an IT professional my face. I however believe that Bynum has simplified it well in his four professional relationships for IT professionals. He states that IT professionals can find themselves in one of four types of professional relationships in the performance of their job. In these relationships, they can find they can have a "significant impact upon the world," and "with such power to change the world comes the duty to exercise that power responsibly." (Bynum) He defines the relationships as:

Employer	-	Employee
Client	-	Professional
Professional	-	Professional
Society	-	Professional

Bynum contends that in the performance of their duties, IT professionals can find themselves in any combination of these relationships, sometimes with conflicting interests. It is therefore important for the professional to have some sort of guide to help recognize these conflicts and to help define a solution to avoid inappropriate behavior. By understanding the many combinations of relationships they may face, and using one of the codes of conduct from any well known organization, the IT professional can ensure that they act in an ethical manner and protect the interests of all parties involved.

CONCLUSION

Since information technology has been a relatively new development in the world of business, it has taken considerable time for the ethical concerns associated with IT to be identified and solutions to be developed. IT has become a significant part of our everyday lives, and without an ethical standard and responsible practitioners, the impact could be devastating to our personal happiness and freedom.

A conundrum exists in IT, in that we have standards that govern the behavior of practitioners, but enforcement is difficult. Many individuals are following the established standards, many even joining professional organizations that are striving to improve IT ethics. But a great number are also using technology to do amazing, and sometimes illegal things, without considering the implications. I find it surprising that many people in IT are committing piracy knowing that it is stealing money form the producers and owners of the data. If they feel that their behavior is not wrong, would they feel the same if it was their product that was being stolen through copying?

Thankfully, there are many professionals and organizations dedicated to improving the ethical state of IT. They have identified the issues concerning privacy, accuracy of information, and the appropriate use of information. They

© SANS Institute 2005 Author retains full rights.

have developed codes of conduct for the professional to follow to ensure ethical behavior. With their growing memberships they are spreading the ideals that will help to advance both the public and inside opinions of the industry. There are many organizations and professionals dedicated to information security and computer ethics alike, and with their insight and devotion we are on our way to a more ethical information community.

© SANS Institute 2005, Author retains full rights.

REFERENCES

Andronache, Tatiana. "Hide and Seek: The Question of Ethics in IT – Part 1." The Galt Global Review. 13 Jan. 2004. 22 Aug. 2004. http://www.galtglobalreview.com/infotech/ethics_in_it.html#focus1

Bartlett, Michael. "Schools Fight Back Against Internet Plagiarism." 6 Sep. 2001. 27 Sep. 2004. Washingtonpost.com. http://www.washingtonpost.com/ac2/wp-dyn/A53402-2001Sep6?language=printer

Bynum, Terrell. "Computer Ethics: Basic Concepts and Historical Overview." Stanford Encyclopedia of Philosophy. 14 Aug. 2001. 25 Sep. 2004. http://plato.stanford.edu/entries/ethics-computer/

"CAI Reasearch." Center for Academic Integrity. 27 Sep. 2004. http://www.academicintegrity.org/cai_research.asp

"CERT/CC Statistics 1988-2004." Carnegie Mellon Software Engineering Institute, CERT Coordination Center. 3 Aug. 2004. 9 Oct. 2004. http://www.cert.org/stats/cert_stats.html

Davis, Gardner. "Ethics Must Come from the Top." Jacksonville Business Journal. 27 Aug. 2004. 4 Sep. 2004. http://jacksonville.bizjournals.com/jacksonville/stories/2004/08/30/editorial1.html

De George, Richard. "Busines Ethics and the Information Age." 22 Mar. 1999. 30 Aug. 2004. http://cyberethics.cbi.msstate.edu/degeorge/

Free-PC.com. http://www.freepc.com/

"Free-PC.com…It's About Time." The Daily Grumbler. 4 Mar. 1999. 29 Sep. 2004. http://jh.pair.com/grumbler-removed/archives/mar0499.htm

"Guidelines and Considerations for Developing a Public Library Internet Use Policy." American Library Association. Nov. 2000. 4 Oct. 2004. http://www.ala.org/Template.cfm?Section=Other_Policies_and_Guidelines&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13098

Lee, J.A.N. "Codes of Conduct/Practice/Ethics from Around the World." 19 Dec. 2002. 9 Oct. 2004. http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/WorldCodes.html#world

© SANS Institute 2005 Author retains full rights.

Mason, Richard. "Four Ethical Issues of the Information Age." Management Information Systems Quarterly 10.1 (March 1986): 5-12. 30 Aug. 2004. http://www.misq.org/archivist/vol/no10/issue1/vol10no1mason.html

"Music industry wins approval of 871 subpoenas." USA Today. 18 July 2003. 25 Sep. 2004. http://www.usatoday.com/tech/news/techpolicy/2003-07-18-riaa-suits_x.htm

Plagiarism.org. 27 Sep. 2004. http://www.plagiarism.org/

Research Papers Online. 27 Sep. 2004. http://www.ezwrite.com/

Standler, Ronald B. "Computer Crime." 4 Sep. 2002. 7 Sep. 2004. http://www.rbs2.com/ccrime.htm

Van Swaay, M. "Computing Ethics: Guiding Principles." 15 Jan. 1997. 25 Sep. 2004. http://www.cis.ksu.edu/Department/ethics.html

"What is Piracy?" Software & Information Industry Association. 25 Sep. 2004. http://www.siia.net/piracy/whatis.asp

© SANS Institute 2005, Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced