Global Information Assurance Certification Paper

Supporting The Ethical Climate Of Information Technology

Overview

A contributing factor to how an industry is perceived is its demonstrated ethical culture. Knowing the right thing to do is not enough; one must also do the right thing. This paper addresses what the information technology community can do to support and ensure the ethical health of its members.

Introduction

It is not enough to judge ethical behavior of information technology (IT) professionals based upon who benefited and who paid. And, when the potential impact of new technology can be both wide-spread and complex, settling for standards based upon the least-common denominator, does not create a strong foundation for IT professionalism. Instead, the IT community must assertively take proactive steps to promote and ensure acceptable behavior from its members.

"Historically, computer professionals as a group have not been overly concerned with questions of ethics and propriety as they relate to computers…Too often, we view computers simply as machines and algorithms, and we do not perceive the serious ethical questions inherent in their use."[1] Some argue that because computers are inert metal and wire, the burden of morality should correctly be assigned to the user. Considering the extent of influence that information technology has on the quality of life, the value of the informational assets it carries, and the potential of more equitably distributing former monopolies on knowledge and insight, both vigilance and safeguards are appropriate at different levels and stations in society. As one strategy, there is growing support for teaching computer ethics early in our children's education as a means of gradually creating "a more responsive and vigilant society that questions the actions taken by computer professionals."[2]

Others recognize that the creators who fashion the technology and those that maintain and secure the technological infrastructure, perhaps, have a more significant responsibility to safeguard ethics and integrity.

> Technology is seen as a "canalization" of social processes: new technical possibilities "invite" new flows in the existing social system…The crucial matter however is to identify those "invitations" that might lead to socially unacceptable consequences, and find out how the social processes can

[1] Denning, Dorothy E., and Denning, Peter J., Internet Besieged: Countering Cyberspace Scofflaws (Addison-Wesley 1998), p.502.
[2] Kizza, Joseph M., "Combating Computer Crimes: A Long Term Strategy" (Dept. Computer Science and Electrical Engineering, The University of Tennessee, 1997) *Abstract,* URL: http://searchpdf.adobe.com/proxies/2/15/84/12.html; accessed 09-02-2001.

> be modified such that these undesirable tendencies do not occur…Instead of leaving the global perspective implicit, and conceiving those broader issues purely as external constraints, computer experts should explicitly deal with these questions, and see them as part of their social responsibility.[3]

Many experts are pondering how ethics should best be applied in the IT profession. Clearly, as facilitators of the transition and guardians of the information age, IT professionals are placed in areas where the boundaries have not been tested. The UK's first professor in computer ethics, Simon Rogerson believes that "The overall goal is to integrate computing technology and human values," he says, "in such a way that the technology advances and protects human values, rather than damages them."[4] Fostering a climate conducive to high professional ethics is all about helping ourselves and others make wiser decisions in difficult situations.

It seems appropriate that computer security professionals should lead the way for establishing ethical practices for the industry. Some say that computer security is a matter of good manners. However, even if all the users employed good manners, there would still be work for computer security professionals to ensure the confidentiality, integrity and availability of their organizations' informational assets. In doing so, security computer professionals can explore how best to address a number of moral or social obligations owed to society, to customers, to organizational management, to coworkers and to the IT profession.

The characteristics of our information assets depend upon the state of computer security. An example of computer security ethical practices can be found with issues fundamental to individual privacy stem from databases having personally identifiable information collected for a particular purpose and with consent. The computer security professional can guard privacy interests by hardening systems against sniffing or cracking and addressing unpermissible data mining through controls over authentication and permissions. Security professionals are also instrumental in ensuring the observance of licensing agreements and intellectual property by physically securing products and monitoring their installation. There are also a number of gray areas outside of the legal bounds that take computer security professionals into uncharted ethical territory. These include monitoring others' computer use, collecting counterintelligence, designing lures, and employing offensive tactics in dealing with hackers.

---

[3] Birrer, Frans A.J., "IT and the Workplace: Perspectives on Technology and the Responsibilities of Experts," *ETHICOMP98-Abstract*, p. 1, URL: http://www.ccsr.cse.dmu.ac.uk/conferences/ccsrconf/abstracts/birrer.html; accessed 09-02-2001.

[4] Middleton, Chris, a conversation with Simon Rogerson, "Ethics Man," p. 2, from article appearing in *Business and Technology* (January 1999), pp. 22-27, republished on-line with permission of Reed Business Information, URL: http://www.ccsr.cse.dmu.ac.uk/staff/mosc/teaching/bandt.htm; accessed 09-02-2001.

It is not the intent of this paper to dwell upon the extent or nature of the social responsibility of computer security specialists, nor IT professionals in general. However, through the responsibilities and experiences in computer security, the IT community can draw upon a foundation of ethical knowledge and practice. The purpose of this paper is to advocate why and how ethics should be implemented and promoted within the IT profession, including computer security specialists. An underlying premise is that adherence to strong ethics, integrity, and social responsibility serves as a cornerstone to the professionalism of all workers in information technology.

Why Should We Be Concerned About Having Strong Ethics In The IT Profession?

Should illegal or unethical employee conduct be proven, the organizational public image, stock price, employee morale or retention may all suffer. Researchers analyzed survey results from 2,293 American workers across major industries and geographically dispersed throughout the country and concluded that

> sound ethics is crucial to keeping employees, especially in a market where nonprofit organizations cannot match private sector salaries and benefits….Employees who believe they work in an ethical environment are six times more likely to be loyal than workers who believe their organization is unethical.[5]

With the shortage of qualified IT workers, the attraction and retention of competent employees may be strong motivation for organizations to conduct an ethical audit or strengthen its ethical stance. Organizations with positive ethical climates can enjoy more loyal and long-term customers and less "lost assets" or "shortages" in inventories and supplies. Organizational productivity improves when employees are treated fairly because they can focus efforts on achieving work results without a conflicting need to solely look out for themselves.

A majority of all participants (59%) in the research described above, believed their employing organization, as a whole, was ethical. The respondent perceptions of the technology industry scored their organizations second to the highest in integrity/ethics. However, the dot.com world has demonstrated notable instances of questioned standards. While ethical judgments may be clear in the abstract, the obligations owed to different groups may conflict in practice. For example, when a failing company sells confidential customer lists, it trades individual privacy owed to customers for corporate longevity owed to stockholders and employees. "In our rise to become the most respected and most powerful country in the world, we might have stretched the skin of our ethics hide….This group (high-tech firms) is rewriting the old standard of ethics."[6]

[5] Smith, Curt, "The Ethical Workplace," *Association Management* (June 2000), v. 52, p. 70.
[6] Murphy, Tom, "Standard of Ethics Remains Critical to Any Business," *Franchising World* (May/June 2001), p. 66.

More than one in four (27%) of the respondent group representing government in the research described above, doubted that senior leaders were people of high integrity. Accordingly, on a scale of integrity/ethical industries, government was rated as the second to the worst. As pointed out by the researchers, this finding is troubling when one considers that government is responsible for monitoring and policing ethical and legal constraints to ensure a free, fair, and democratic society. Government is also responsible for regulating aspects affecting the IT profession, such as anti-trust, bandwidths, computer crime, standards for Federal government computer security and intellectual property.

Regardless whether other studies would still reveal a lack of government credibility on ethical issues, professionals should not rely upon government regulation for ethical inspiration or instruction. Solely relying upon government efforts to reduce misconduct or ethical lapses is insufficient to promote widespread observance of ideal standards of ethics and professionalism in the technology industry and in the IT workers that facilitate it.

One, however, should not undervalue the power of legislation and regulations to influence behavior. Laws and rules, by their impact, are proscriptive in defining what we shall not do without consequences. As such, they generally do not prescribe the expected, nor ideal, behavior. In essence, their enforcement sets the least common denominator.

As the media regularly reveals unacceptable and illegal business practices committed by employees, struggling technology start-ups, and Fortune 500 firms and to mitigate illegal employee acts, the 1991 U.S. Sentencing Commission Guidelines were issued and amended. The Guidelines govern the sentencing of corporations for federal crimes and recognize that properly implemented corporate compliance programs may be considered for substantial reduction of criminal penalties if illegal conduct is proven. In response, many corporations have established such programs, including careful review of their codes of ethics.

The Guidelines for the corporate compliance program offer sound and concrete definitions. An "effective program to prevent and detect violations of law" means a program that has been reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct. The hallmark of its effectiveness is that the organization exercises due diligence in seeking to prevent and detect criminal conduct by its employees and other agents.[7] Corporate “due diligence” requires at a minimum that the organization must have:

---

[7] 2000 Federal Sentencing Guidelines, Section 8A1.2, Application Instructions, Commentary, Application Notes, 3(k), URL: http://www.ussc.gov/2000guid/8a1_2.htm; accessed 09-14-2001.

1) established compliance standards and procedures, reasonably capable of reducing the prospect of criminal conduct.
2) specified high-level individual(s) with overall responsibility to oversee compliance with such standards and procedures.
3) used due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities.
4) taken steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by training or disseminating publications that explain what is required.
5) taken reasonable steps to achieve compliance with its standards, e.g., by monitoring, detecting and auditing, as well as a reporting system whereby employees and other agents could report criminal conduct by others within the organization without fear of retribution.
6) consistently enforced through appropriate disciplinary mechanisms for offenders and individuals responsible for the failure to detect an offense.
7) after an offense has been detected, taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses -- including any necessary modifications to its program.

Neither the reduction of exposure to liability (i.e., risk control), nor the minimization of potential consequences (i.e., risk management) should be the driving force for organizations to tone up their standards of conduct and establish compliance programs. The risk of legal implications is among other variables contributing to how corporations and employees view what is good or right.

Employees, themselves, must not adhere to integrity values for fear of being caught in illegal activity. Instead, they should be able to rely upon a professional standard of behavior that would enable them to identify appropriate choices and to resist the temptations to participate in unethical or illegal activities—regardless of the potential of forbidden fruits. "Professional self-preservation alone cannot be the sole motivator for the pursuit of ethical policy. It is based solidly on the precept that we must be able to make determinations and judgments about the righteousness of our action. Ethics provides us with a framework for making those judgements."[8] And, although each IT professional may already have values and ethical ideals, perhaps it is incumbent upon the IT profession to provide the environment and support for ethical advocacy and practical guidance for application in the work setting.

[8] Morgan, Sean, "Ethics and Legalities: What's the difference?" *Information Security Reading Room* (November 22, 2000), URL: http://www.sans.org/infosecFAQ/legal/ethics.htm; accessed 08-27-2001.

What Activities Contribute To Ensuring A Strong, Ethical Profession?

It is not enough to endorse the notion of having an ethical profession, nor is it sufficient to leave ethical judgments by IT workers as they occur. IT professional ethics are a necessary framework for accountability and appropriateness consisting of a set of rules, values, standards and moral obligations that govern the conduct of computer professionals and the principles used with computers and the information they produce.

A number of endeavors in combination with a statute-driven environment can promote the kind of atmosphere necessary to ensure ethical practice and to lessen the temptations to cut ethical corners. Although a great deal of ethical conduct will overlap that required through legal codes, the former seeks compliance with both the letter and the spirit of the law. These additional efforts to support professional ethics also set a baseline upon which IT workers can cultivate individual commitment to actively raise and safeguard a higher expectation of the level of integrity in their practice.

Practicing ethics is a critical leadership and management responsibility within any industry. Various activities in the IT and other occupations have demonstrated success and should be promoted to ensure wide-spread practice of ethical conduct. These include developing and widely communicating a Code of Ethics; integrating a variety of options supporting ethical training and reinforcement for IT professionals; and, monitoring and enforcing ethical standards within the IT community.

1. **Develop And Widely Communicate A Code of Ethics.**

Ethical codes are typically drawn around broad principles that set moral obligations, values, and ideals to which members should aspire. A useful code of ethics for IT professionals is one that offers practical guidance in an environment of changing technologies and roles, prioritizes responsibilities to aid in resolving conflicts, and is as inspirational as it is instructional. It would, indeed, be a tall order to develop all-encompassing standard and expect universal endorsement. Even the acceptance of the priorities of core values may evolve as leaders, ethics proponents, pragmatists and thinkers contribute their insights and experiences to form a body of knowledge specific to the IT industry. Over time, a general consensus can emerge regarding what behavior should be expected under certain circumstances, as well as generally accepted practices of professionalism and integrity.

We must also recognize the need to widely gain consensus without allowing a reduction to platitudes, excessive flexibility, or vagueness to replace practical, brightline guidance.[9] Sticky issues left unaddressed because of the difficulties in

[9] Schwarz, Bart, The Nuts and Bolts of an Effective Compliance Program," *HR Focus (*August, 1997), v. 74, p. 13.

garnering agreement in their handling are likely to surface and then cast shadows upon the ethical proponents and drafters of materials for not applying adequate due diligence in identifying and initially addressing potential problems.

"A difficulty is that along with a policy vacuum, there is often a conceptual vacuum…What is needed in such cases is an analysis which provides a coherent conceptual framework within which to formulate a policy for action."[10] As the IT profession evolves, the accumulation of experience and wisdom will yield more robust case studies, analysis of key issues, and practical guidance. Presently, there is already a growing plethora of literature on ethics and codes of conduct for computer professionals that is a foundation for identifying and substantiating appropriate behavior.[11] It will require active participation in fostering the ethical climate and applying the growing body of ethical knowledge in the IT context by the members of the IT community before self-imposed professional standards can become the norm.

Prominent international and national IT professional associations, such as the Association of Computing Machinery (ACM), the British Computer Society (BCS), the Canadian Information Processing Society (CIPS), the Data Processing Management Association (DMA), and the Institute for Certification of Computer Professionals (ICCP) have led the way in adopting association codes of ethics. There are many similarities among these codes in the obligations to society, employer, clients, colleagues, organization and the profession. However, an advocate for a single, coherent code of professional conduct organized along the above described constituencies to which the IT professional has obligations, concluded that there was an apparent flaw after his review of these codes: "the lack of priorities among the subjects of moral obligations."[12]

A collaboration by ACM and the Institution of Electrical Engineers (IEEE) Computer Society produced a Software Engineering Code of Ethics and Professional Practice that delineates priorities among the various obligations. The first principle in this Code guides the developer to consider all stakeholders, not just the software engineer's employer or client. The second principle of due respect, addresses the protection of human values and states that the primary concern in all decisions is the public interest. The Code asserts the priority of concern for the public well being over loyalty to the employer or profession.[13]

---

[10] Moor, James H., "What is Computer Ethics? A Proposed Definition," p. 2, URL: http://www.ccsr.cse.dmu.ac.uk/staff/Srog/teaching/moor.htm; accessed 09-02-2001.
[11] Tavani Herman, Editor and Vance David, Maintainer, Codes of Conduct for Computer Professionals (CPSR 1996), URL: http://cyberethics.cbi.msstate.edu/biblio; accessed 09-02-2001.
[12] Oz, Effy, "Ethical Standards for Information Systems Professionals: A Case for a Unified Code," *MIS Quarterly* (December 1992) pp. 423-433.
[13] Gotterbarn, Donald and Miller, Keith, "Maturing Standards and the Current Software Engineering Codes of Ethics" (June 4-5, 1999), p. 4, URL: http://infoeagle.bc.edu/bc_org/avp/law/st_org/iptf/commentary/…/1999060403.htm; accessed 09-

Other associations, such as the American Society for Information Systems (ASIS) recognize "the plurality of uses and users of information technologies, services, systems and products and the diversity of goals or objectives, sometime conflicting, among vendors, producers, mediators, and users of information systems."[14] The Ethics Codes of the Association of Ethical Internet Professionals (AEIP) recognize serious moral and ethical obligations to the public, fellow members and the association, as well as advise members to be honest in all business and professional relations, and to follow and support the Golden Rule.[15]

"Codes of ethics and case studies need each other. Without guiding principles, case studies are difficult to evaluate and analyze; without context, codes of ethics are incomprehensible."[16] Some codes of ethics are instructive by specifying the responsibilities for fair information practice, such as that of the Computer Professionals for Social Responsibility and Privacy International (CPSR);[17]other organizations, such as the Computer Ethics Institute are somewhat proscriptive, but also address "consideration and respect for your fellow humans."[18]

Regardless of the presentation, style or arrangement of standards of ethics, codes bring value when the principles embodied are reinforced by the proponent organizations. Publications and messages advocating strong, ethical practice from leading IT experts, professors, certifying organizations and association officials are powerful tools of communication. When communicated widely and with demonstrated support, a number of benefits can be achieved, in addition proactively demonstrating self-regulation.

> Codes serve to educate, both prospective and existing members of a profession about the shared commitment of the members of a profession to undertake a certain quality work and the responsibility for the well being of the customer and user of the developed product….Codes also serve as indirectly educating the public at large about what the professionals consider to be a minimal acceptable practice in that field, even if practices by a non-professional…As we have seen, the Code encourages the

---

02-2001 (The IEE Rules of Conduct can be found at http://www.iee.org.uk/Profdev/Guides/conduct.htm; accessed 09-02-200).

[14] Code of Ethics, American Society for Information Systems (ASIS), URL: http://csep.iit.edu/codes/coe/ASIS_Code.htm; accessed 09-02-2001.

[15] The Ethics Codes of the Association of Ethical Internet Professionals (AEIP), URL: http://www.aeip.com/ethics-f.html; accessed 08-27-2001.

[16] Center for Study of Ethics in the Professions, Illinois Institute of Technology, "Using Codes of Ethics," Codes of Ethics Online, p. 3, URL: http://csep.iit.edu/codes/coe/Users_guide.html; accessed 09-02-2001.

[17] Computer Professionals for Social Responsibility and Privacy International, Code of Fair Information Practices, URL: http://csep.iit.edu/codes/coe/CPSR_Code.htm; accessed 09-02-2001.

[18] Computer Ethics Institute (a project of the Brookings Institution), "The Ten Commandments of Computer Ethics," URL: http://cpsr.org/program/ethics/cei.html; accessed 08-27-2001.

professional to do positive actions. The Code also [sic] the professional resist pressures to act unethically.[19]

2. Integrate A Variety Of Options And Programs Supportive Of Ethics For IT Professionals.

Clearly, the simplest and quickest way to ensure a strong ethical community is to recruit and involve more ethical people. Ethical surveys and audits are available and could be promoted or customized for each IT specialization; however, many situations will not be covered. If one assumes that ethics is something that must be put into people before they can be professionally responsible, then programs need to identify the operable values and be rules-based with penalties for non-compliance. Values reflect something that is widely accepted as being consistently worthwhile. As such, they serve as an anchor for determining the right thing to do. The rules-based aspect of a program further aids in the development of skills in applying the proper value in the right situation. The fear of penalties promote compliance with the preferred behavior.

Often the ethical challenge, however, is how to best apply familiar values to novel business situations. In some cases of ethical breach, the problem stems from a lack of ethical perception, rather than a lack of values. If one assumes that people already have values that must be brought out of them, then programs need to aid ethical decision making by sensitizing professionals of the likelihood that most of their decisions will have an ethical component that should be considered. By developing ethical decision making skills or integrity-based approaches, employees are enabled to become self-policing.

The key is to present and reinforce a clear, practical message that knowing the right thing to do is not enough; one must also do the right thing. To foster and reinforce a strong ethical environment supporting this message, the IT community needs a combination of awareness, training and educational activities, such as ethics courses, ethics modules in specialized courses, publications, case studies, certifications, and mentoring programs. These activities and programs should form a life-long continuum of professional development options that not only sustain improvement of individual ethical understanding and application, but also promote a healthy ethical climate for the IT community.

Universities are creating separate computer ethics courses and codes of ethics in addition to integrating ethics modules into the computer science programs.[20] Research in ethics education suggests positive results from integrating ethics training into core courses. However, one researcher found the longevity of

[19] *Op. Cit.*, Gotterbarn, Donald and Miller, Keith
[20] Center for Study of Ethics in the Professions, Illinois Institute of Technology, "Computing and Information Systems," *Codes of Ethics Online*, URL: http://csep.iit.edu/codes/coe/Users_guide.html; accessed 09-02-2001.

improvement from such training to be short-lived. In this research, the subjects' ethical standards dissipated over a four-week period after their exposure.[21] However, other researchers[22] have empirically confirmed benefits of ethics integration into component specialty courses along with active learning approaches, including "involvement of professional associations in developing classroom materials and training professors in their use."[23] Therefore, a variety of additional activities supporting ethics awareness, training and education must be available to IT workers, regardless of their stage of mastery of technological skills or IT experience.

Associations, academics, and certifying organizations can make a significant contribution through sponsoring and publication of research, studies, and materials supporting strong ethics in the IT community. For example, the collection and dissemination of actual and hypothetical case studies would be helpful in garnering member participation and endorsement. Aids in establishing an ethical baseline include additional commentaries on the application of ethical values and explanations of the reasoning used to conclude whether the described behavior under the particular factual context would be considered either ethical or acceptable in the IT community. Over time, a collection of these commentaries would reflect the collective wisdom, offer detailed guidance, identify best practices, support appropriate behavior by both students and IT workers, and aid the public in understanding what it should expect from the IT community.

The value of certification in the IT specializations is rapidly appreciating. "The mere presence and visibility of these certificates has come to confer the attribute of 'credibility' on the bearer. The various certifications mean that they are 'officially' recognized by an association appropriate to their industry."[24] Some certifying organizations build adherence of its code of ethics as part of the certification and its subsequent renewal. For example, ISCA Labs requires computer network professionals to sign an ethics statement that points out that "not only is it important for all network security professional to adhere to the principles expressed in this Code, each certified individual should encourage and support adherence by other certified individuals."[25]

Establishing meaningful ethical standards demonstrates that members certified in the profession understands the importance of their role in society and are willing to assume their professional responsibilities in a manner that also recognizes

---

[21] Richards, Clinton, "The Transient Effects of Limited Ethics Training," *Journal of Education for Business* (Jul/Aug, 1999), v. 74, no. 6, p. 332.
[22] McNair, F. and Milam, E. E., "Ethics in Accounting Education: What is Really Being Done." *Journal of Business Ethics* (1993), v. 12, pp. 797-809.
[23] Richards, *Op. Cit.*, p. 333.
[24] Brecher, Hugh, "Trust Begins Here," *AEIP Online Article*, p. 2, URL: http://www.aeip.com/trust-begins-here-f.html; accessed 08-27-2001.
[25] ICSA Security Practitioner Certifications, TruSecure Corporation, URL: http://www.trusecure.com/html/secsol/practitioner.shtml; accessed 09-04-2001.

moral obligations owed to members of society. In addition to making an initial ethical commitment by affixing a signature to a code of ethics, additional requirements strengthen the professional development and value of the certification.[26] For example, potential certificants should participate in an ethics component in the certification training and testing. Prospective certificants could also be required to demonstrate baseline ethical competency, perhaps through employer or personal references. Certification renewal could be made contingent upon completion of mandatory continuing education credits that include ethics or participation in activities that support integrity-based, professional conduct.

The benefits from coaching and mentoring have increasingly gained the attention of management and educators as the techniques and approaches continue to become refined. Promoting good mentoring skills and practices among association members and students, not only stimulates collegiality but also, encourages a level of intellectual interchange and consensus. Including discussion of ethical issues, along with sharing of technical knowledge, increases the level of sensitivity to ethical implications of given situations and to the needs of, and effects upon, others. By building in opportunities for open discussion of problems and approaches into mentoring programs and forums, participants who encounter ethical dilemmas or circumstances stemming from conflicting interests or priorities will have a safety net to probe for acceptable options.

3. Establish A System For Monitoring And Enforcement Of Ethical Standards Within the IT Community.

Professional associations and other IT-related organizations have a range of opportunities to gauge and even, monitor the ethical climate of the industry. In addition to being a source for communicating guidance and case studies and offering forums for collegial discussions regarding ethical conduct and conflicts, some associations in various occupational areas support a hearing panel for complaint reporting, review or appeal, and a means to dispense sanctions against violators.

Associations and certifying organizations have the power to expel ethical offenders through enforcement of their codes of ethics. For example, $(ISC)^2$ advises information systems security professionals that their certification is a privilege that must be both earned and maintained. Certified individuals intentionally or knowingly violating its four ethical canons will be subject to action by a peer view panel.[27] The canons are to protect society, the commonwealth, and the infrastructure; to act honorably, honesty, justly, responsibility, and legally; to provide diligent and competent service to principals; and, to advance and protect the profession.

---

[26] Peluso, Steven T., "Planning Professional Certification Programs," *Association Management* (May 2000), v.52, no. 5, pp. 65-67.

[27] $(ISC)^2$ Code of Ethics, URL: http://www.isc2.org/cgi/content.dgi?page=31; accessed 09-02-2001.

Although specific disciplinary standards need not be defined in advance, a formal procedure for review and determination of punishment from a schedule of penalties is essential for enforcing and reinforcing professionalism. A continuum of sanctions and penalties might include private warnings; public reprimands; probation, suspension or termination of memberships; probation, suspension or revocation of certifications, as well as imposed special conditions for prevention or remedy, such as required ethical training or professional service.

Enforcement of proper ethical behavior by associations and certifying groups should be considered part of the educational process for the individual violator, as well as for the IT industry. Unlike the impact of government regulations, such systems of enforcement administered within the IT community may not have long-term control over the behavior of individual members. Instead, the offering of models and incentives, expanded resources, advocacy and support for professional development and ethical practice, promote a stronger, stable and highly respected IT community.

Summary

A contributing factor to how an industry is perceived is its demonstrated ethical culture. IT professional ethics is a framework for accountability and appropriateness consisting of a set of rules, values, standards and moral obligations that govern the conduct of computer professionals and the principles used with computers and information they produce.

The benefits of an industry that has earned a strong ethical reputation through its professional conduct are many. Researchers have found that organizations with positive ethical climates enjoy more loyal and long-term customers, less "lost assets" or "shortages" in inventories and supplies, easier attraction and retention of competent and loyal employees, and high productivity. Through corporate compliance programs, organizations also find value in reducing their exposure to legal liability, as well as minimizing potential consequences and penalties should illegal conduct be proven.

The IT community should be concerned with cultivating and maintaining a strong ethical atmosphere for its members. Essential support for professional ethics should be assumed by IT associations, certifying officials, academia and members of the IT industry as part of a critical leadership and management role. In tandem with a statute-driven environment, an ethical climate can be fostered through a combination of programs and activities for life-long ethics development and reinforcement. Members of the IT community must understand that it is not enough to know the right thing to do, but that they must also do the right thing as professionals. Strategies can be implemented to promote the kind of atmosphere necessary to ensure ethical practice and to lessen the temptations to cut ethical corners. These include developing and widely communicating a Code

of Ethics; integrating a variety of options supporting ethical training and reinforcement for IT professionals; and, monitoring and enforcing ethical standards within the IT community.

Sources For Further Information

Charles H. Calhoun and Mary Ellen Oliverio, "Self-Assessment of Your Ethics Environment," *The CPS Journal* (January 1999), v. 69, no. 1, p. 54-55.

Ethics Code of Association Of Ethical Internet Professionals - An International association of web businesses committed to ethical business practices as defined by an ethical code of conduct. URL: http://www.aeip.com/ethics.html

An Informative Interactive Question and Answer Page on Internet Ethics, Computer Ethics, Cyber Ethics, E-Commerce Ethic - An Informative Interactive Question and Answer Page on Internet Ethics, Computer Ethics, Cyber Ethics, E-Commerce Ethics, Web Ethics and Other General Ethical Issues. URL: http://members.aol.com/internetethics

Legalethics.com: The Internet Ethics Site - Legalethics.com offers the legal profession links and references to ethics rules, regulations, and articles relating to the integration of the Internet into the practice of law. URL: http://www.legalethics.com

Online Ethics Center: Ethics of Internet Use - Ethics of Internet Use Related Materials maintained by the Online Ethics Center Instructional Resources in Engineering Ethics, Computer Ethics and Research Ethics. This page has links to other sites and information about their contents. URL: http://www.onlineethics.com/keywords/int

Rogerson, Simon and Prior, Mary, "Is IT Ethical?", 1998 ETHICOMP Survey of Professional Practice, The IMIS's Column on Computer Ethics, *IMIS Journal* (February, 1999), p. 1, URL: http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv9nol.html

Security Issues on the Internet - Ethics on the Web - Ethics on the Web would seem to be the last topic to be covered in a technical discussion of the Internet. But, as with any democratic society, the Internet depends on agreed-upon rules of behavior to survive as the computer era evolves. URL: http://www.echonyc.com/~ysue/ethics.html

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor