**ETHICS AND THE INFORMATION SECURITY PROFESSION**

Whether you subscribe to a professional code of conduct[1] or you just claim to be the "good guy" who is protecting the information assets of your organization, your colleagues, your employer, and those whose information you protect expect you to behave ethically. In this context, I use ethics to mean "the rules or standards governing the conduct of the members of a profession."[2] However, elements of its common use as a synonym for morals also apply. Ethical conduct includes both acts of commission and acts of omission. We have obligations to perform certain tasks and obligations not to perform others. Just as a soldier may be held to account for accepting an unlawful order, so may the information security professional be held to account for acceding to management requests if they would violate professional ethics. I have found, however, a wide diversity of opinion among people who assert professional status in our field.

The use of "social engineering" as a technique for testing security, for example, is viewed by some as ethical and by others as unethical. Since I have a background in applied psychology where psychological experimentation might have included "tricking" a person, I have strong feelings about the protocols that you should follow. I believe that a full and professional debriefing of any victims of such trickery is needed. Otherwise, the security test may inadvertently harm these people. In most situations I've heard about, no such protocols were in place. I'd view such testing as unethical. I recognize, however, that other competent and well-meaning professionals may hold a contrary opinion. The rules in our profession are evolving with few well-documented cases.

Many organizations with which we may associate have codes of conduct. The Information Systems Security Association (ISSA) has a terse one (see <http://www.issaintl.org/members.html>). The Information Systems Audit and Control Association (ISACA) has a longer one, which also refers to additional ISACA standards (see <http://www.isaca.org/cert3.htm>). And the Association for Computing Machinery (ACM)[3] has a very detailed code (see <http://www.acm.org/constitution/code.html>). The International Information Systems Security Certification Consortium, (ISC),[2] also has a code of ethics. It is only slightly longer than the ISSA code. At the time of my writing, the Ethics Committee of (ISC)[2] was revising this code. In the discussion that follows, I will refer to these and other codes of ethics.

[**SOME BEHAVIOR IS CLEARLY UNETHICAL**](http://web.a.ebscohost.com/ehost/delivery?sid=a1bdf6c5-1714-4b39-9b32-416ed47f142c%40sessionmgr4009&vid=13&hid=4101&ReturnUrl=http%3a%2f%2fweb.a.ebscohost.com%2fehost%2fdetail%2fdetail%3fvid%3d12%26sid%3da1bdf6c5-1714-4b39-9b32-416ed47f142c%2540sessionmgr4009%26hid%3d4101%26bdata%3dJnNpdGU9ZWhvc3QtbGl2ZQ%253d%253d#toc)

When the issue is selling confidential data to which you have privileged access or mounting a denial of service attack against a previous employer who refused to renew your employment contract, the information security professional has little trouble knowing what is, and what is not, ethical behavior. Shades of gray invade our ethical palette when we must weigh a social good against a personal evil, or when we can only accomplish one of mutually exclusive objectives forcing an ethical dilemma. For example, an employee tells you of an overheard conversation in which "George" boasts of a scheme to defraud his employer. You have the authority to turn on detailed auditing for all of his transactions and the privileged access level necessary for reading his e-mail, should you investigate George to determine the truth of the allegation? Can you ignore the warning? What if George was boasting of a bomb he had built instead of a fraud he was going to commit? What if George had been discussing only a novel he had just read?

The Hippocratic Oath taken by medical doctors includes a pledge to do no harm. Perhaps we should begin with this ethical edict. (In fact, the ACM code contains a similar pledge.) Simple as this principle sounds, our actions in complex situations force us to make difficult choices. We are bound to weigh the interests of many parties in our professional activities. For example, how will our action (or inaction) affect our employer, other employees, stockholders, vendors/suppliers, customers, our professional colleagues, and society at large? Whose interests should take precedence when an inevitable conflict occurs? Although many of us have years of risk management experience and may have used risk analysis tools to assist us, our experience with ethical assessments may lie more with our personal character than with any training in ethical analysis. Our codes of conduct tend to speak in absolutes, but we tend to operate more on the basis of situational ethics. In our earlier example with George, does the risk to the many outweigh the rights of the few? Or are personal freedoms an absolute? If you feel that this begins to sound like a political or religious discussion, then you grasp the complexity of determining ethical behavior. When we truly wish to act ethically, real-world cases may force difficult choices. When we need to determine if someone has acted ethically, for example, in enforcing a professional code of conduct, we may similarly face difficulties, both in knowing what the ethical action should have been and in knowing whether the professional's actions were unethical or just poor judgment.

As information security professionals, we may need to meet a higher standard than other information professionals. Because we have "special knowledge" others will rely on our advice. If our advice proves inaccurate, we must take responsibility for it. Even when our advice is accurate, because we will not always succeed in making our case clear or sufficiently convincing, some people will ignore our advice. Is a "CYA" memo to the file expiation for us when damage results from our being ignored? Should it be a defense in an ethics proceeding?

None of the codes of ethics I've read address the resolution process for ethical dilemma. For example, a requirement to protect confidential information (or a national security classified document) may make cooperation with an investigation difficult, if by cooperation we mean the volunteering of such information. Some of the codes require compliance with "professional standards" as yet undocumented for the information security profession. And all of them ask us to make judgments about outcomes when we can only accurately assess our own actions. In this last case, we seem to ask members of our profession to foresee all consequences. I believe the lack of specificity -- in particular, the absence of clearly documented standards of behavior --makes self-regulation problematic. Notwithstanding, I propose a few rules that might spark a debate.

1. I will resign rather than participate in unethical conduct.

The practical implications of ethical practice include a willingness to resign rather than participate in unethical conduct. If your management insists on you monitoring the actions of an individual or group, for example, to catch them at "something" so management can fire them, such monitoring may be unethical -- even illegal -- especially if no objective reason to suspect them of wrongdoing exists. Your first obligation would be to advise management of the risk such an action entails. But if management insists, you are forced to choose between ethical conduct (i.e., you refuse to participate) or unethical conduct (i.e., you do as asked).

2. I will report unethical conduct to appropriate authorities.

Refusing to participate may be insufficient in meeting your professional obligations. If you have a mechanism for independent reporting of fraud and abuse, you may also have an obligation to report the actions of your management.

3. I will support my colleagues in their ethical conduct.

The information security professional may face difficult choices. Unethical behavior should have consequences to the professional, although ethical behavior is no talisman warding off adverse results. Other members of the profession have an obligation, in my view, to support the ethical conduct of their colleagues. Conversely, we should refuse to engage professionally with persons known by us to conduct themselves unethically.

4. I will shun those persons whom I know have conducted themselves unethically.

One of the hallmarks of a profession come of age is its ability to police itself. To the extent that the bodies promoting professional certifications in our field take seriously this obligation, our endeavors rise to the stature of a traditional profession. If we do not take seriously our professional ethics, we risk externally imposed regulation or the denigration of our field to that of a technical specialty, an administrative function, or a hired hand.

Our professional ethics warrants wider discussion and open debate. Codes of conduct are a good start, but we need a body of professional standards. Perhaps we may also be able to develop "ethics analysis" tools to assist us. Much work in academic circles has already been done. See, for example, the Center for Applied Ethics at <http://www.ethics.ubc.ca/resources/computer/index.html>. You may also wish to see a wide variety of codes of ethics from many fields (including a "hacker" code of ethics!). If you visit <http://www.ethics.ubc.ca/resources/professional/codes.html> you, will find more than two dozen.

Please let me know your views on codes of conduct and professional ethics. You may send me an e-mail at rspoore@ralphs-poore.com.

[**Notes**](http://web.a.ebscohost.com/ehost/delivery?sid=a1bdf6c5-1714-4b39-9b32-416ed47f142c%40sessionmgr4009&vid=13&hid=4101&ReturnUrl=http%3a%2f%2fweb.a.ebscohost.com%2fehost%2fdetail%2fdetail%3fvid%3d12%26sid%3da1bdf6c5-1714-4b39-9b32-416ed47f142c%2540sessionmgr4009%26hid%3d4101%26bdata%3dJnNpdGU9ZWhvc3QtbGl2ZQ%253d%253d#toc)

1. For examples, the Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Protection Professional (CPP), or Certified Fraud Examiner (CFE).

* 2. The American Heritage Dictionary of the English Language, New College ed. (Boston: MA, Houghton Mifflin Company.)
* 3. ACM has a special interest group for security audit and control (SIGSAC) that participated in creating its code of ethics.

~~~~~~~~

By Ralph Spencer Poore

RALPH SPENCER POORE is an Area Practice Leader, Electronic Commerce for Ernst & Young LLP.

Copyright of Information Systems Security is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.

**References**

Poore, R. S. (1999). Ethics and the information security profession. *Information Systems Security*, *8*(1), 15.