Ethics in Information Security
the Higher Standard

Michael E. Whitman, Ph.D., CISM, CISSP
Kennesaw State University
Ethics in Information Security

Ethics: define socially acceptable behavior
Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these

Ethics and Education

Overriding factor in leveling ethical perceptions within a small population is education
Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
Proper ethical training vital to creating informed, well prepared, and low-risk system user
Deterrence to Unethical Behavior

Deterrence: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls

Laws and policies only deter if three conditions are present:
- Fear of penalty
- Probability of being caught
- Probability of penalty being administered

Codes of Ethics

Several professional organizations have established codes of conduct/ethics

Codes of ethics can have positive effect; however, our profession does not require its professionals to be a member of any particular organization.

It is the responsibility of security professionals to act ethically and according to codes of ethics, the policies of employer, their professional organization, and the laws of society
ACM

The Association of Computing Machinery was established in 1947 as “the world's first educational and scientific computing society”

Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property

(ISC)$^2$

The International Information Systems Security Certification Consortium, Inc. Is an organization focused on development and implementation of information security certifications and credentials

Code primarily designed for information security professionals who have certification from (ISC)$^2$
(ISC)² Ethical Canons

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

SANS

The System Administration, Networking, and Security Institute is a professional organization dedicated to protection of information and systems

Code of Ethics focuses on Respect for:
- The Public
- The Certification
- My Employer
- Myself
SANS Code of Ethics

Respect for the Public

- I will accept responsibility in making decisions with consideration for the security and welfare of the community.
- I will not engage in or be a party to unethical or unlawful acts that negatively affect the community, my professional reputation, or the information security discipline.

ISACA

Information Systems Audit and Control Association is a professional association with focus on auditing, control, and security

ISACA concentrates on providing IT control practices and standards
ISACA Code of Ethics

Members and Certification holders shall:

2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.

3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority.

[...]
ISSA Code of Ethics

I have in the past and will in the future:

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities that might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.

WestPoint Cadet Code of Conduct
Ethical Issues in Computer Use

- IP Violations
  - Illegally used/copied software
  - Illegally copied/shared music
  - Illegally copied movies
  - Plagiar
- Fraud, waste and abuse in computer use
- Hacking

IP Use

Copyright law specifies “fair and reasonable use” for IP including:
- Legal backup for software, movies and music.
- Legal copying and use of broadcast media
- Legal use of published works
In the beginning…

Hacker:
a computer enthusiast,
someone who enjoyed pushing the
boundaries of computer technologies, and
who frequently had to apply unorthodox
techniques to accomplish their desired goals.

Modern Definition

Hack:
– “Informal To alter (a computer program): hacked
  her text editor to read HTML.
– To gain access to (a computer file or network)
illegally or without authorization: hacked the firm's
  personnel database.”

http://dictionary.reference.com/search?q=hacking
Problem Foundation

Fascination with “Outlaws”
Hackers Portrayed in the Media (cont)

Good Guys and Bad Guys
The Black Hat Conference

“The Black Hat Briefings are a series of highly technical information security conferences that bring together thought leaders from all facets of the infosec world – from the corporate and government sectors to academic and even underground researchers. The environment is strictly vendor-neutral and focused on the sharing of practical insights and timely, actionable knowledge. Black Hat remains the best and biggest event of its kind, unique in its ability to define tomorrow’s information security landscape…”

The Black Hat Conference (Cont)

“Black Hat Founder and Director Jeff Moss is also the founder of DEFCON, the largest and best-known hacker conference in the world. In 2007, DEFCON celebrated its 15th anniversary. The experience and connections created by 15 years at the intersection of network security and hacker ingenuity is what makes Black Hat the one-of-a-kind conference it is, one where the establishment and the underground are equally at home.”
The “Ethical Hacker”
oxymoron – “a figure of speech by which a
locution produces an incongruous, seemingly
self-contradictory effect.”
http://dictionary.reference.com/browse/oxymoron

Hacker a la (ISC)2
“a hacker was originally a person who sought to
understand computers as thoroughly as
possible. Soon hacking came to be
associated with phreaking… which is clearly
illegal.”

Hacker a la (ISC)2

“Malevolent hackers attempt to penetrate systems for fun or profit through the use of self-developed or open-source hacking tools. After a successful penetration, they may introduce other vulnerabilities into the system, such as a backdoor, to provide easier access. Crackers, on the other hand, are focused on breaking security measures within software for their enjoyment or profit. Their activities are primarily conducted to break copyright protection methods incorporated into software packages.”


“Hacker Ethics” a la Steven Levy

“promotes the belief of individual activity over any form of corporate authority or system of ideals.”

Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-On Imperative!

All information should be free.

Mistrust Authority—Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.”

The Dilemma

Ethical -
1. pertaining to or dealing with morals or the principles of morality; pertaining to right and wrong in conduct.
2. being in accordance with the rules or standards for right conduct or practice, esp. the standards of a profession.

http://dictionary.reference.com/browse/Ethical

Point of the Rant

Choose your terms carefully.
– If a police officer shoots a criminal in the line of duty, is it “legal murder”?

The difference between a hacker and an information security professional is…

AUTHORIZATION
The Information Security Professional

Information security professionals are expected to be above reproach as the true guardians of the organization’s information assets. Any doubt as to our true beliefs, motives and ethics undermines the efforts of us all.

The Higher Standard

We as ethical computer users must BE, KNOW, DO:

• BE examples of higher ethical standards
• KNOW the codes of ethics, policies, laws and regulations applicable to our professions
• DO the right thing all the time… including strict enforcement of standards…
Thank You For Your Time

Michael E. Whitman, Ph.D. CISM, CISSP
Director
KSU Center for
Information Security Education
mwhitman@kennesaw.edu
http://infosec.kennesaw.edu