Ethics and Security

ISSA International Ethics Committee

V2.1 4/27/07

Importance of Ethics to Security

- Information Security professionals are entrusted with the crown jewels of an organization.
- Ethical behavior, both on and off-the-job, is the assurance that we are worthy of that trust.
- IS Security sets and upholds a standard
  - Corporate Ethics programs originating from the CSO
  - Promote uniform adherence to policy through example

Topics

- Ethics in the Information Security Realm
- ISSA International Ethics Posture
- ISSA International Ethics Committee
- Importance of Ethics To Security
- Responsibilities of Security Professionals

Ethics Overview

- Ethics is about how we ought to live*
- The purpose of Ethics in Information Security is not just philosophically important, it can mean the survival of a business or an industry**

Ethics is doing the right thing,
even when no one is looking

ISSA International Code of Ethics (Part 1)

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;

ISSA International Code of Ethics (Part 2)

- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities which 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.

ISSA's Posture – Ethics for the Security Professional

- Set Ethical Standards for Membership
  - Include Broader Audiences
- Educated and Informed Members
  - Case Studies, Articles, Courses
- Universally Applicable Standards
  - Geographically, Culturally
  - Cross Discipline

ISSA International Ethics Committee

- Founded in 2002
- 15 active members
- Purpose: Provide guidance on ethical behavior for Information System Security professionals, develop and maintain guidelines for ethics relating to Information Security practices.

Proactive Promotion and Education to Influence Positive Behavior

Accomplishments

- Approved policy by ISSA International Board
  - Reporting and reviewing ethical complaints, appeals
- Respond to and hear valid ethics complaints
  - Time-sensitive
  - Confidential
  - Unbiased
  - Consistent analysis of facts and perspectives
  - Findings referred up to ISSA International Board
- New Disclosure of Relationships Process
  - Identify and mitigate potential Conflicts of Interest
  - Completed forms are reviewed and suggestions provided
  - ISSA International Board, ISSA Foundation, Ethics Committee
- Articles for ISSA Journal, Outreach and Education
- Ad-hoc research

ISSA Ethics Complaint Handling

- Formal, Written Complaint is Received and Verified for Completeness
- Notices sent to both parties
  - Complete Complaint
  - Copy of Policy, Clear Description of Next Steps
  - Listing of Ethics Committee members (ability to recuse members – eliminate bias)
- Evaluation of Facts as Submitted by Both Parties
  - Some Clarification may be Requested
  - Mediation Assistance may be Requested
- Hearing Panel Assembled – Conference Call Scheduled
  - At least 3 members of the Committee (Voting)
  - A member of the ISSA International Board (Voting)
  - Include a current Chapter Officer (Voting)
  - Association Attorney (Non-Voting)
- Findings and Recommendation Sent to ISSA International Board

Ethical Challenges in InfoSec

- Misrepresentation of certifications, skills
- Abuse of privileges
- Inappropriate monitoring
- Withholding information
- Divulging information inappropriately
- Overstating issues
- Conflicts of interest
- Management / employee / client issues

Ethical Challenges – Snake Oil

- “Consultants" who profess to offer information security consulting, but offer profoundly bad advice
- "Educators", both individuals and companies, that offer to teach information security, but provide misinformation (generally through ignorance, not intent)
- "Security Vendors", who oversell the security of their products
- "Analysts", who oversimplify security challenges, and try to upsell additional services to naïve clients
- "Legislators", who push through "from-the-hip" regulations, without thoughtful consideration of their long-term impact

Some Resource Links

http://ethics.csc.ncsu.edu/

http://www.ethicsweb.ca/resources/

http://ethics.iit.edu/index.html

http://onlineethics.org/

On the development of a personal code of ethics...

http://www.domain-b.com/management/general/20060401_personal.html

Corporate ethics training...

http://www.integrity-interactive.com/

http://www.easyi.com/enus/business-ethics/solutions.asp

On the role of ethics...

http://securityawareness.blogspot.com/2005/07/role-of-ethics-in-information-security_07.html

http://www.seifried.org/security/index.php/Closet20000531_Ethics_in_Information_Security

Something from the SANS Reading Room

http://www.sans.org/rr/whitepapers/legal/54.php

Ten Commandments of Ethics in Information Security

Thou shalt not use a computer to harm other people.

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

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

Thou shalt not use a computer to steal.

Thou shalt not use a computer to bear false witness.

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

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

Thou shalt not appropriate other people's intellectual output.

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

Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

-Courtesy of the Computer Ethics Institute,
A project of the Brookings Institution

Questions/Discussion