The status of codes of security ethics

At the RSA conference this year, there was an ethics panel made up of the heads of the 5 families of information security; ISACA, ISC2, ASIS, SANS, and ISSA – certifiers all. Based on what they said and the ethics standards they have in place for their members, as of 2007, the information security ethics situation as we see it is poor at best. Here are some key issues:

- No ethicists are apparently involved in the development of ethics for these groups.
- Ethics standards are based on avoiding liability to the society and cultural relativity.
- Internal attempts to meet standards such as those of the IEEE and other professional societies have failed, resulting in less prescriptive and less specific standards.
- Ethics standards largely ignore the well being of society and other people in favor of keeping the individual employed and benefiting the management team.
- A self-declared counsel for Microsoft indicated that ethics only matter when you are in a tight spot and the panel largely agreed.
- One questioner indicated that they experimented on other peoples' computers without their prior permission and the panel members did not find fault.
- The societies do not use situation ethics examples to train their members.
- Sanctions of members are rare and difficult to get through, and accusers often back down when they learn that there is a validation process in place for complaints.
- The panel members failed to apply or identify elements of their standards in analysis of ethical issues presented, and violated those standards in their opinions of issues.
- None of these societies has taken an ethics stand on issues of privacy or surveillance.
- These societies have not yet tried to reconcile their standards against each other.
- These codes have little to say about situations commonly experienced in the field.

The ethical standards of these societies appear to be lacking. If the executives in charge of those standards don't apply them in a public forum, we cannot reasonably expect their members to apply them in private at risk of their livelihoods. Detailed examination of these codes of ethics yields many serious questions as well. There is a long way to go. Codes of ethics that seem far more advanced and appropriate include the IEEE, ACM, and Software Engineering codes of ethics. The security organizations are starting to seek to change this.

FCA largely follows the IEEE code of ethics owing to its propriety in almost every area, its relative brevity clarity, and its foundation in a highly respected field with acceptance on a global basis. In addition, FCA has uniformly applied contractual elements for each worker that identify specific elements of ethical behavior encountered in security contexts and give explicit rules on their application. Failure to follow these rules strictly is immediate grounds for termination and violators have been consistently terminated on first violations. Each worker is given a detailed individual review of these upon hiring and periodic reviews of key issues prior to each effort undertaken for each client. This awareness program helps assure that clarity is achieved for all workers for each task they are given prior to the start of their efforts on that task and serves to reiterate these principles when and as they are most needed. Team members also discuss the many ethical issues we encounter in the field as they arise to get a group consensus around what to do in each case. Ethical dilemmas are the nature of security.

