Global Information Assurance Certification Paper

The Ethics and Legalities of an Investigative Incident Response Policy

Sean Morgan

Ethics and Legalities: What the difference?

Webster's unabridged dictionary defines ethics as: "The study of standards of conduct and moral judgment;" Ok, we can probably all agree on that. If you don't, philosophy professors at your local institution of higher education are probably prepared to hold forth on that simple subject for hours on end. Personally, I've sat through a few of those sessions myself. Nevertheless, why do we as aspiring or practicing security professionals care about ethics?

The answer, of course, is that establishment and adherence to a common code of ethics is a defining characteristic of a 'profession'. It is a hard and fast requirement if you desire to be certified by the $(ISC)^2$ as a CISSP. They have an established code of conduct. If you "knowingly violate any provision of the Code [you] will be subject to action by a peer review panel, which may result in the revocation of certification." This language certainly makes it appear that they mean business on this point and I, for one, don't doubt them. If you want to be in this profession or any other, you can expect to adopt and adhere to codes of conduct.

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 actions. Ethics provides us with a framework for making those judgments.

Some of our philosophy professors might argue: that in a hypothetically ethical society there would be no need for laws or legalities. They may be right, but you and I don't live in this hypothetical society. If we did, we certainly would be in other lines of work. Hackers wouldn't hack, thieves wouldn't steal, politicians wouldn't lie and employees wouldn't wile away hours of their time surfing through inappropriate material on the Internet.

At a fundamental level, this is why we have laws. Our societies and communities adopt laws to maintain order and force acceptance of certain standards of conduct. In the United States, certain of these laws apply to how employers and employees must behave. The nature of most laws, however, is that they usually set minimum standards of acceptable conduct and prescribes penalties for failure to meet those standards.

What I will be arguing for in the remainder of this paper is the adoption of higher ethical standards for conducting incident investigations within an organization with the goals of:

- A fair and accurate reporting of facts and events
- Reasonable respect and sensitivity for an individuals sense of privacy
- Maintaining a high morale within the organization and fosters an environment of cooperation with information security

The fundamental difference between legality and ethics is this:

Legality deals with the basic question of: *Can we do something?*
Ethics deals with the question of: *Should we do something?*

What are the legalities?

Legally and generally speaking, employers have quite broad powers in investigating suspected abuse or compromise of their systems. That means that we; as security professionals, auditors and investigators; have the legal ability to make suspected wrongdoer's lives miserable.

If a company or organization has provided some basic general policies declaring the computers, information and telecommunications systems to be their property along with the information they contain; they can rummage through an employees computer files provided they could provide a valid business reason for doing so.

According to a Privacy Rights Clearinghouse fact sheet on employee monitoring the following activities are in general allowed:

- Employer monitoring of phone calls
- Employer maintenance and acquisition of phone records
- Employer monitoring of what's on a computer screen
- Employer monitoring and review of e-mail

To make an even better case of doing these things employers will often place logon banners on their systems advising users that monitoring activities take place and use of systems implies consent to this monitoring.

In 1988, Congress passed the Employee Polygraph Protection Act of 1988. This legislation was aimed at limiting an employers ability to administer polygraph tests and use the results in employment decisions.

There are, however, exceptions to this act that grants employers exemptions for these rules. The exceptions to the law include: public sector employees, national defense and security issues, employers conducting and ongoing investigations of economic loss or injury, employers that are involved a business dealing with controlled substances and employers providing security services.

In the investigation of security incidents, I find the exemption for the ongoing investigations of economic loss to be quite interesting. It seems quite plausible that employers can make, with relative ease, a case that information security breaches have some economic loss associated with them. It isn't fair to disparage this piece of legislation because it does provide protections for employees and spells out clearly for employers what steps have to be followed for exemptions to be applied. Most all of these requirements do make things better for an employee taking such a test.

Employees are not without rights. Employees may claim that their files and data are protected by asserting that they have a reasonable expectation of privacy. However, in the face of a reasonably clear policy described briefly above, this sort of an assertion is hard to make.

These legal issues of privacy are still quite contentious and unlikely to be settled definitively any time soon – if indeed they are ever settled clearly.

Still, there are things that employers are clearly not allowed to do under the law. An employee may make a case against an employer for invasion of privacy if employers engage in any of the following tactics:

- Deception
- Violation of confidentiality
- Secret, intrusive monitoring
- Intrusion into an employees private life

Where should our ethics lead us?

It bears repeating that laws set minimum standards. It is clear, therefore, that any security professional conducting an investigation especially an internal investigation should not violate any laws in doing so. This stills leaves the question of: What should an investigator do that goes beyond these minimum standards?

This question practically screams for a policy. That is the core purpose of policy, after all. Policy establishes rules and guidelines for what should and should not be done. Having an incident investigation policy provides us an opportunity to raise the standards for conduct above the ground floor issue of legality. Policies provide us an avenue to express our ethics and accomplish goals that transcend the minimalist need to maintain order – it gives us a chance to aspire to greater goals.

I laid out some of those goals earlier but want to present some concepts that I believe can be incorporated into an incident investigation policy to help accomplish these goals:

- A statement disavowing the use of the investigative process to further personal goals of investigators or individuals reporting alleged violations.
- A statement describing how an investigation may be initiated and upon whose authority it may be started.
- A statement describing appropriate reporting of investigative findings.
- An admonition to investigators not to discuss or disclose details of an investigation outside of reporting or conducting the investigation along with consequences for violating this confidentiality.
- A statement that anyone under investigation is to be extended the assumption of innocence until proven guilty and that as such reasonable steps will be taken to protect their reputation.
- A statement that holds investigators personally and professionally responsible to conduct fair and honest appraisals and to inform subjects that such accountability exists.
- A statement providing the subjects of internal investigations the ability to appeal to higher levels of management to raise and settle disputes about perceived breaches of privacy.

All of these actions, and perhaps others that should be included, go beyond the minimal requirements of the law. They help to provide reassurances to investigative subjects and other observers in the organization that these investigative efforts are concerned with truth and fact and do not represent 'witch hunts' or indiscriminate random searches. As conscientious professionals, we don't have time for such nonsense. We may as well say so up front and make our fellow employees more comfortable with our roles and how we intend to conduct them. Failing to do so may reflect badly on our chosen profession and us.

International Information Systems Security Certification Consortium, "(ISC)^2 Code of Ethics, URL: http://www.isc2.org/code.html

Privacy Rights Clearinghouse, "Employee Monitoring: Is there privacy in the workplace?", Fact Sheets, November 2000, URL: http://www.privacyrights.org/fs/fs7-work.htm

Barbara Kate Repa, "Legal Actions Against Privacy Violations", Nolo's Legal Encyclopedia, 2000, URL: http://www.nolo.com/encyclopedia/articles/emp/privacy.html

Barbara Kate Repa, "Computers and Email on the Job: They're Watching You",

Nolo's Legal Encyclopedia, 2000, URL:
http://www.nolo.com/encyclopedia/articles/emp/computers.html

United States Department of Labor, "29CFR801 – Application of the Employee Polygraph Protection Act of 1988", Code of Federal Regulations Pertaining to ESA, March 4, 1991, URL:
http://www.dol.gov/dol/allcfr/ESA/Title_29/Part_801/toc.htm