In the first of this three-part series, Becki True, CISSP and I recounted the story of the breach of security of the colemanforsenate.com Website. This second column is also the product of close collaboration between Ms True and myself.

** * * *

What would have been the ethically correct decision in this case, and how can we know that it is ethically correct? The first stage of an ethical decision filter asks if our action violates laws <http://www4.law.cornell.edu/uscode/>. Did the other players in this incident of full disclosure break any laws? We are not lawyers, and am not qualified to provide legal advice, but 18 USC 1030(a), the Computer Fraud and Abuse Act of 1986 <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030-000-.html> states that

> “Whoever— (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— (a) information contained in a financial record of a financial institution, or of a card issuer” is subject to fines and jail time. “The term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.”

From this reading, we take it that the person(s) who downloaded the database seems to have violated 18 USC 1030(a).

In contrast, Attorney Jennifer Granick<http://cyberlaw.stanford.edu/profile/jennifer-granick> is the Civil Liberties Director at the Electronic Frontier Foundation<http://www.eff.org> and the Executive Director of the Center for Internet and Society<http://cyberlaw.stanford.edu> at Stanford Law School. According to her, neither Richards nor Wikileaks.org broke the law. “Based on her knowledge of this case, as well as the law, Granick said it was legal for Richards to view the Web directory on which Coleman’s donor list resided. “There has to be some kind of indication that information is locked away,” she said.”<http://minnesotaindependent.com/29067/wikileaks-it-pro-not-in-any-danger-in-coleman-leak-lawyer-says>

The next stage is to ask if your actions comply with the rules of the profession. Are there standards in the IT profession that were violated here? Many IT certifications and associations, especially those related to the security field do have such codes of ethics:

- (ISC)2 <http://www.isc2.org/ethics/default.aspx>
- EC-Council <http://www.ecouncil.org/codeofethics.htm>
- SANS <http://www.sans.org/resources/ethics.php?ref=3781>

In our opinion a code of ethics should be required for all IT certifications, so all IT practitioners...
can be aware of the ethics of our profession. In our opinion, an IT professional should have taken action to notify the administrators of the Coleman Website that there was a problem and sensitive information was vulnerable to exposure rather than exposing the vulnerability in public.

Normally, we also ask if our proposed action would be embarrassing if it were revealed to the public; in this case, the answer for the principals was clearly “No.” However, we can state categorically that we would be ashamed of revealing someone else’s vulnerability in public without intensive good-faith efforts to get the problem fixed. [MK adds, “When I discovered a major hole in Hewlett-Packard’s MPE operating system in 1982, I reported it to headquarters, not to the press – and would have done so even if I had not been working for HP.”]

Another classic question is the categorical imperative: if everyone behaved as we are proposing, would we approve of the result or not? For example, we could ask how we would feel if a Website we managed were found in this state. Would we want to be notified or would we want someone to post the vulnerability on public Websites and to publicize it on social networking sites? And what would the consequences be if every vulnerability in every system were immediately broadcast to the public without time for correction? Would we approve of this state of affairs or prefer a different approach?

Another part of ethical analysis is “Cui bono?” Whom does our behavior benefit? When there is a disjunction between the benefits and the harm in an action, we should examine the proposed course of action carefully.

Yet another question that helps us analyze ethical dimensions of a decision is to raise the question of instrumentality: are we treating other people respectfully and kindly as individual human beings whose feelings and interests we are considering in our decision or are we treating them as objects or instruments toward a personally useful end? In this case, it seems to us that not informing the people who had bad security was neither respectful nor kind.

We hope that this analysis helps readers apply the principles of ethical analysis to their own situations.

For more reading on this subject, see

- The extensive bibliography about full disclosure maintained by the Wilderness Coast Public Libraries in Monticello, Florida <http://www.wildernesscoast.org/bib/disclosure-by-date.html>.
One final note: one of us [MK] did contact Adria Richards and found her to be a charming, intelligent and thoughtful information technology professional. We sent these articles to her before publishing them to be sure that she would not find them offensive. We wish her well in her continued professional career.

* * *

Becki True, CISSP is a graduate student in the MSIA Program at Norwich University. She welcomes your comments.<mailto:becki@beckitrue.com>

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Becki True & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.