I recently received the following interesting letter from a reader who has kindly permitted to quote it:

> I work for one of the largest cities in the United States. Due to the tightness of the budget, there is a plan to use computer science student interns to setup and manage the network security for various city agencies. Most of these agencies do not currently have the expertise or resources to dedicate to security.

I feel that it is a very bad idea for many reasons. There will be no oversight of the intern's work. Moreover it doesn't help the agencies become anymore security-savvy when the internship ends. I am also uncomfortable with the idea that the age bracket that is most common to hack is the same as most of these college interns. So, while the interns will have the knowledge to tighten security, this knowledge could also be used to leave/create backdoors that will be hard to find. I guess I am concerned about their lack of vested interest in the agencies and the lack of possible accountability. Am I out of line?

I would like the city to think of all of the consequences of this proposal before it goes into affect. I sense it could have the potential to be PR and security catastrophe.<

I responded that the reader’s concerns seem very reasonable. In addition, I wrote, I'd add to the memo that the system _could_ work and be a wonderful opportunity for both the students and the city if

* the students are vetted using detailed phone conversations with their academic references;

* each candidate is interviewed to discuss their attitudes towards hacking and to evaluate their maturity;

* they write logs and prepare weekly reports on their findings and their actions so that others can learn from them;

* they provide teaching sessions at the end of their projects where they summarize the lessons learned and leave a permanent record of their work;

* the students are supervised by their college professors in weekly status meetings;

* clear policies are in place on acceptable use of city resources;

* all the students understand to whom they are reporting in their work so that there is no confusion about lines of responsibility;
* all the permanent staff understand to whom the students report for the same reason as the previous point.

As a university professor myself, I think that internships are a wonderful way for both the employer and the students to learn; in addition, the students’ reports can serve as case studies (with suitable masking of sensitive information) for lectures by the students and as fresh material for professor’s lectures.

My own experience with many university students interested in security is that they are committed to genuine security, not to childish hacking games. The criminal hackers either don’t have the discipline to excel in university studies or they are very good at fooling their professors into believing that they’re not criminal hackers.

Finally, I note that the NSA and NSF cyber-security scholarship programs, in which Norwich students have particularly distinguished themselves by winning an unusually high number of seats, include summer internships in government departments. Clearly somebody thinks that college students can be a real security asset.

* * *

For further reading about NSA and NSF cyber-security scholarships:

National Science Foundation <http://www.ehr.nsf.gov/due/programs/sfs/>


* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 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.