Journal of International Technology and Information Management

Volume 22 | Issue 4 Article 4

11-4-2013

# The “Ethics” of Teaching Ethical Hacking

Ronald E. Pike
*California State Polytechnic University, Pomona*

# The "Ethics" of Teaching Ethical Hacking

**Ronald E. Pike**
**College of Business Administration**
**California State Polytechnic University, Pomona**
**USA**

## ABSTRACT

*Programs teaching ethical hacking are growing steadily. The argument for teaching ethical hacking focuses on the need to better understand attacks and attackers. However, some believe that teaching offensive hacking skills increases risk to society by drawing students toward criminal acts. The proponents of teaching ethical hacking argue that ethics training permeates related curriculum providing students with ample preparation to understand the risks and choose healthy behaviors. This paper examines mechanisms beyond classroom-based curriculum to minimize the risk of students committing criminal acts with the skills acquired in an ethical hacking course.*

## INTRODUCTION

Hacking grew out of a tradition of mutual cooperation among software developers to create software projects that were innovative, aesthetic and included some form of technical virtuosity (Levy, 1994). As computer communications became pervasive with the rise of the Internet the term hacker was also used to describe the process of exploring and experimenting with computer networks (Sterling, 1993). However, as commercialized use of software and computer networks grew they became property with putative boundaries and crossing these boundaries became criminalized. For the purpose of this paper the terms white-hat and black-hat hacker will be used. A white-hat hacker is defined as a hacker who is committed to full compliance with legal and regulatory statutes as well as published ethical frameworks that apply to the task at hand. A black-hat hacker then is a hacker who either ignores or intentionally defies legal or regulatory statutes with presumably little interest in ethical frameworks.

In academic programs the open use of software and networks are often encouraged and even required as students work to fulfill course requirements. Students then find themselves working in partnership with other students on shared projects in much the same manner as early hackers. However, at other times the sharing of code and systems is not allowed. Students are typically informed when resources can be shared and when they cannot with little demand for students to make decisions about whether or not it is appropriate to share information or access other's systems. It is unclear that academic training environments provide students with an environment where they gain experience applying ethical practices. This paper stems from a discussion of whether students are being offered appropriate supports and experiences to help them make informed ethical decisions when applying information security training. Student expulsions and convictions for hacking activities are on the rise and indicate that more needs to be done to protect students (Cox, 2013; Schwartz, 2012).



ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

## ETHICAL HACKING

Courses teaching ethical hacking have been gaining popularity over the past decade with a growing number of schools getting involved. Curriculum related to such courses typically includes related training in ethics and law as well as a call for professors to model appropriate behavior with respect to ethical hacking. Risks related to teaching such classes is often addressed by noting that "… students who learn traditionally illegal computing skills in the course of studying computer security will use those skills for the greater good far more often than they will use them illegally or immorally (Pashel, 2007, p. 199)." When focusing on protecting society from the illegal actions of students than this answer is perhaps adequate, however, it is important to note that teaching hacking creates two separate risks. There is a risk to society if a student misuses the skills they are taught in addition to the risk to students in the program who may be drawn into illegal activity through the training received.

Protecting students is particularly important as they are often unaware of the seriousness of their actions with respect to hacking. A recent study revealed that both white-hat and black-hat hackers understand the consequences of illegal hacking, however, college students do not. The study notes, "Hackers are keenly aware that if one were caught engaging in illegal hacking activities, his/her life would be seriously disrupted. This shows the success of the United States government in communicating the seriousness of engaging in illegal hacking activities to the hacker community. Meanwhile, the college student population is not getting the same message (Young, Zhang, & Prybutok, 2007, p. 285)." There is also a significant concern as to whether students gain the experiences they need to understand how to effectively apply the ethics training that is part of ethical hacking programs.

## METHODOLOGY AND DATA COLLECTION

### *Methodology*

A search of the literature revealed little guidance in preparing students to responsibly use hacking skills learned in college aside from the ethical hacking literature which has been in place for more than a decade. Three senior information security professionals were recruited as Subject Matter Experts (SMEs) and asked what training or set of experiences would assist college students in understanding and applying ethical training related to hacking. Each of the three SMEs holds the position of Chief Information Officer or Chief Information Security Officer and they routinely hire and assess the performance of information security professionals. The SMEs recommended an information collection from a broader set of professionals and rejected the idea of a specific questionnaire for interviews as there was insufficient information on which to base specific questions. Instead, they recommended that information security professionals be allowed to respond without prompts with what they believe would help college students seeking careers as information security professionals avoid illegal activities. Furthermore, the SMEs recommended that only the "low hanging fruit" be pursued which was determined to mean items recommended by at least 25% of respondents.



ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

All of the interviewees were self-proclaimed information security professionals with more than one year of experience. A total of 206 interviews were conducted at three information security conferences in the Southwestern United States in the spring of 2013. One of the events was open to all information security professionals, one was specific to the motion picture industry and required an invitation and credentials to attend and one was specifically geared to CISOs and also required an invitation and credentials for attendance. There were 122, 35 and 49 respondents respectively from the three events.

While less than 15% of the respondents classified themselves as hackers, all of the respondents worked full-time in the information security industry. Each of the respondents was familiar with hacking and dealt with it in capacities that ranged from policy development, training, auditing, managing and practicing in the information security field.

Respondents were asked for their names, company affiliations, positions in their company, and years of experience in the information security field. Participants were also asked whether they thought ethical hacking should be taught as part of a cybersecurity program at the university level and then were asked for any recommendations for helping students to heed ethical guidelines presented in the certified ethical hacking literature.

### *Data Collection*

If the respondent met the study criteria then they were asked for recommendations on activities that would help understand and adhere to ethical guidelines. Responses were combined into categories that were determined after the data was collected when similar responses were grouped together. Following the advice of the SMEs, any recommendation category receiving at least 25% support from respondents was included and examined further through academic literature.

All 206 interviewees believed that ethical hacking should be included in cybersecurity courses at the university level and most of the interviewees offered one or more recommendations for protecting students. The recommendations were grouped into categories and four of these categories met the 25% inclusion threshold. Each of these four categories was actually recommended by 80 (39%) or more respondents and are shown below:

- Social interaction/support system
- Competition
- Recognition
- Ongoing skills development

Each of these four areas was explored through the academic literature to seek specific recommendations which are offered in this paper. Three additional categories were created that failed to reach the 25% inclusion threshold yet they each had 22 (10%) or more respondent recommendations which were:

- Interaction with cybersecurity-related law enforcement
- Cybersecurity internships
- Student attendance at meetings and conferences of professional cybersecurity organizations

While these latter three categories did not meet the 25% cutoff for inclusion in this paper, each was mentioned by more than 10% of respondents which meets a base level of significance so they are listed here but not examined further. The remainder of the manuscript is focused on the four categories that were identified by 25% or more of respondents as recommendations for protecting students that participate in an ethical hacking course.

## DISCUSSION AND PROPOSITIONS

### *Social Interaction*

Study respondents mentioned the need for positive social groups more often than any of the other recommendations. Group affiliation and teamwork is evident on both sides of the cybersecurity field (white-hat and black-hat hackers) and the importance of these affiliations is clear. There is a seemingly endless list of groups on the white-hat side including many CERTs (Computer Emergency Responses Teams) the ECSG (European Cyber Security Group) the HITRUST Cyber Security Working Group and many more. Groups of black-hat perpetrators likely maintain a low profile but the groups of which we are aware, such as Anonymous, make it clear that groups of mutual support are import to criminal hackers as well. A Google search for "cybersecurity group" yielded nearly 7,000 hits so there is a large array of such groups. Such affiliations are likely a valuable way for white-hat and black-hat hackers to share technical knowledge and build skills; however the importance of such affiliation clearly goes deeper.

White-hat hackers who believe in the rule of law form communities of practice that help in creating ethical frameworks to guide activities within the discipline. Peer groups and social support systems are used to both guide technical innovation and also learn to deal with difficult legal and regulatory issues in ways that are lawful and in compliance with the groups adopted ethical framework. Black-hat hackers who believe their cause (political, environmental, monetary, etc…) supersedes the rule of law form into affinity groups with others who have morally justified the deviant behavior of the group (Young et al., 2007).

It is clear in all of the reviewed literature that white-hat and black-hat hackers are concerned with acceptance of their actions among their peer groups. An action is likely to be taken if it is considered to be morally acceptable to ones peer group (Young et al., 2007). The social identity theory states that participation in a social group will cause an individual to make choices that fall along a continuum between their own personal choice and choices the group deems appropriate. Furthermore, the self-categorization process indicates that members of an organization will categorize options into those that fit with the group consensus and those that fall outside of the group consensus (Hogg & Terry, 2000). Therefore, an individual will not only be influenced by their peer group, they are also likely to accept the group's categorizations such as legal actions

being acceptable and illegal actions being unacceptable. So if the group does not accept a particular action, then group members are likely to avoid that action.

> Proposition 1: The creation of student peer groups that support white-hat hacking practices, with ethical and moral codes that are guided by the rule of law, will reduce the likelihood of student engagement in unethical activities.

### *Competition*

Competitions appear to have etched a significant role for themselves in the cybersecurity education landscape. There are numerous papers that espouse the learning innovations and advantages made possible through cybersecurity competitions (Carlin, Manson, & Zhu, 2008; Conklin, 2005; White, Williams, & Harrison, 2010). Comments provided by respondents in this study supported the value of cybersecurity competition in strengthening student skills. However, this paper focuses only the role of cybersecurity competitions in reducing potential criminal behavior among students involved in ethical hacking training.

While a review of the literature did not reveal a direct connection suggesting that competitions may support adherence to ethical guidelines, there are several indirect positive influences. Perhaps the most notable of these is the fact that cybersecurity competitions give many students their first real look at what the working world may bring. The competitions themselves along with the related career fairs and industry involvement create an excitement for the opportunities ahead, many of which would be lost as a result of a criminal conviction. Also, many competitions offer "real-world" scenarios that will force participants to consider the ethical and legal implications of their actions. In some cases students are required to present ethical issues or dilemmas to a panel of industry professionals which provides invaluable experience applying the ethical training that comes from ethical hacking courses. Feedback after such an event can also help students understand where their zeal to successfully complete a task in competition may have caused them to cross an ethical or legal boundary.

Additionally, cybersecurity competitions allow students to interact with one another and industry professionals expanding the social interactions available. As students realize the scope of the community that is accessible to white-hat hackers the strength of such social interactions will have an even greater influence on their behavior. Finally, competitions have a powerful acculturation effect which will help students to better understand the two clear categories they must choose between in cybersecurity. Competitions that are run by organizations espousing white-hat hacking have a wonderful opportunity to help students view the contrast between the white-hat and black-hat sides of the cybersecurity industry with a focus on the benefits of white-hat hacking and the dangers of black-hat.

> Proposition 2: Integrating cybersecurity competitions into academic programs provides numerous learning benefits, experience implementing and testing legal/ethical training and opportunities for social networking that will extend the reach and effectiveness of peer support groups mentioned in proposition 1.

### *Recognition*

The need of hackers to gain recognition for their talent and accomplishments was identified by the industry respondents as being very important for many within the hacker community. Hackers join a community in part for mutual support but also a desire for recognition within the community (Wark, 2006). This desire for recognition runs deep in the hacker community and the inability to gain recognition through white-hat hacking activities may drive students toward black-hat activities. Recognition can come in the form of doing well in a competition but it can also come from monitoring and tracking student activities on learning materials and classroom activities in addition to competitions and other external activities.

Leaderboards or scoreboards have long been used in sports venues to identify the performance of competitors. This same mechanism is already being used in the National Cyber League (NCL) and other cybersecurity competitions. Similar leaderboards within academic programs can allow students to understand how their skills stack up against others and provide recognition for high achievers.

> Proposition 3: Providing recognition for white-hat hacking activities that are relevant to an individual's peer group will reduce the likelihood that a student will need to engage in black-hat activities to gain recognition and will reinforce the value of the white-hat activity.

### *Ongoing Skills Development*

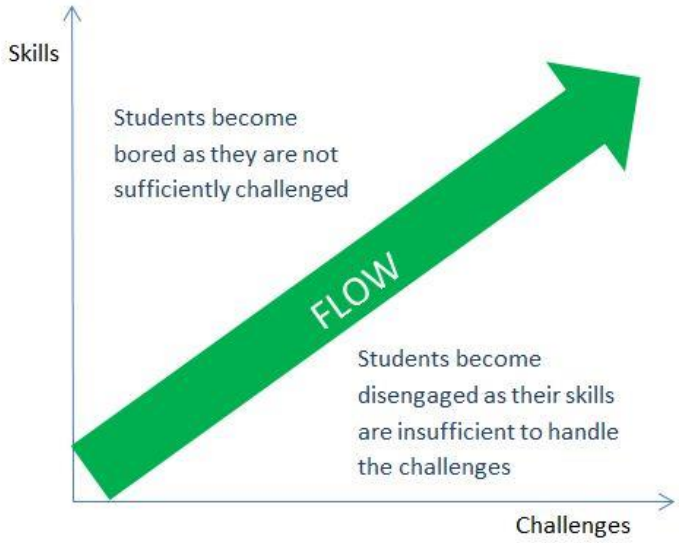
Ongoing skills development is a critically important issue for hackers. A hacker is a purveyor of innovative and elegant solutions which means that maintaining the status of a hacker requires a relentless commitment to taking on and mastering ever increasing challenges. Hackers enter a state of flow, a term from the communications literature that means actions freely and almost effortlessly move from one to the next (Voiskounsky & Smyslova, 2003). Flow is considered to be an internal motivator that is reached as a participant faces challenges at the cutting edge of his or her skill level and then successfully manages the challenge. Video games are an excellent example as participants will play for hours facing challenge after challenge not even realizing the passing of time in the process and with no reward other than the internal gratification related to the task and perhaps some bragging rights within the participant's social group.

For academic programs this means there is a need to be prepared to increase the challenges to meet and continually build the skill levels of students. Figure 1 illustrates the continuum of challenges required to ensure students have sufficiently simple tasks at the start of the learning process and sufficiently difficult tasks as their skills development process matures. Partnerships between academic institutions as well as relationships with government and industry may be important components in maintaining an adequate level of challenge for students. Such relationships could consist of learning projects, research projects, competitions, internships and more.



ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

**Figure 1: Relationship of Skills vs Challenges.**




Adapted from Voiskounsky and Smyslova, 2003

Proposition 4: Providing challenges that are properly matched with students' skill levels will serve to reduce the likelihood that students will turn to black-hat activities. Sufficiently simple tasks also may help in retaining students who do not enter a state of flow because their skills are insufficient to successfully handle the challenges they are facing.

## LIMITATIONS

It should be noted that interviewing security professionals at conferences may have influenced outcomes as topics such as mutual support and competitions were being presented at the conferences. However, it is the belief of this author that this influence is not problematic as the presentations were not influenced by the study and are simply an added indication of the importance of these topics to the cybersecurity field.

## CONCLUSIONS

With unanimous support from 206 industry professionals it is clear that cybersecurity programs must consider the role that ethical hacking will play in their programs. However, it is also important to carefully consider risks to students and methods of mitigating these risks. Teaching ethical hacking is a serious responsibility given the destructive power of the skills being taught and the allure of negative influences on students. This is especially true when the cybersecurity challenges students face during and after their academic programs are complex and it is often difficult to determine how to properly apply the ethics training received in courses. There is an ethical requirement for educators to do all we can to ensure students are prepared for the challenges they will face with the skills we provide.



ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Both the interviews with industry professionals, and a review of the literature, reveal that teaching students the value of professional networks and getting students engaged with a supportive peer group is critical. Recommendations for the development of peer groups that offer support to students, and ideally a connection with industry associations and relevant law enforcement agencies, is an important next step in the effort to protect students in ethical hacking courses.

The role of current best practice in teaching ethical hacking (teaching ethics, warning students of criminal penalties and modeling ethical behaviors) is critically important. However, properly constructed social interactions and support, competition, recognition and sufficient challenges can augment efforts to help students avoid criminal activity while also enhancing cybersecurity programs.

## REFERENCES

Carlin, A., Manson, D., & Zhu, J. (2008). Developing the cyber defenders of tomorrow with regional Collegiate Cyber Defense Competitions (CCDC). *Proceedings of the 25th Information Systems Education Conference, ISECON 2008, November 6, 2008 - November 9, 2008*, 25. Association of Information Technology Professionals.

Conklin, A. (2005). The use of a collegiate cyber defense competition in information security education. *Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD '05, September 23, 2005 - September 24, 2005* (pp. 16–18). Association for Computing Machinery. doi:10.1145/1107622.1107627

Cox, E. (2013, January 24). Ahmed Al-Khabaz expelled from Dawson College after finding security flaw | Canada | News | National Post. *National Post*. Retrieved June 30, 2013, from http://news.nationalpost.com/2013/01/20/youth-expelled-from-montreal-college-after-finding-sloppy-coding-that-compromised-security-of-250000-students-personal-data/

Hogg, M. A., & Terry, D. J. (2000). Social Identity and Self-Categorization Processes in Organizational Contexts. *Academy of Management Review*, *25*(1), 121–140.

Levy, S. (1994). *Hackers: Heros of the Computer Revolution*. New York: Penguin.

Pashel, B. A. (2007). Teaching students to hack: ethical implications in teaching students to hack at the university level. Proceedings of the *2006 Information Security Curriculum Development Conference, InfoSecCD '06, September 22, 2006 - September 23, 2006*, 197–200. Association for Computing Machinery. doi:10.1145/1231047.1231088

Schwartz, M. (2012, August 31). Accused LulzSec Hackers Attended College Together - Security -. Retrieved June 30, 2013, from http://www.informationweek.com/security/attacks/accused-lulzsec-hackers-attended-college/240006598

Sterling, B. (1993). *The Hacker Crackdown*. New York: Bantam.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-Based model of computer hackers' motivation. *CyberPsychology & Behavior, 6*(2), 171–180.

Wark, M. (2006). Hackers. *Theory, Culture & Society*, *23*(2/3), 320–322.

White, G. B., Williams, D., & Harrison, K. (2010). The CyberPatriot national high school cyber defense competition. *IEEE Security and Privacy*, *8*(5), 59–61. doi:10.1109/MSP.2010.166

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281–287.

# This Page Intentionally Left Blank



ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy