This is the second of a two-part series on hiring hackers and criminal hackers into information technology (IT) groups as programmers, network administrators and security personnel.


Chapter 12 of the CSH5 is “The Psychology of Computer Criminals” by Dr Q. Campbell and David M. Kennedy. The authors point out that research on computer criminals suggests that some criminal hackers may exhibit addictive or compulsive behavior resulting from “a combination of compulsive behaviors and curiosity.” In addition, “the need for power and recognition by their peers may both be motivating factors for some cybervandals. Computer criminals report feelings of enjoyment and satisfaction when they prove themselves better than system administrators and their peers.”[p 12.3]

In another section, the authors report research that suggests that criminal hackers may “alter their thinking to justify their negative actions…. Immoral behaviors can be justified by comparing them to more egregious acts, minimizing the consequences of the actions, displacing responsibility, and blaming the victim[s] themselves.”

Another problem is that some criminal hackers may exhibit traits associated with clinical personality disorders such as the narcissistic personality disorder.<http://www.mekabay.com/ethics/totem_taboo_cyber.pdf> One of the most important aspects of this disorder is the sense of entitlement. Campbell and Kennedy write, “Entitlement is described as the belief that one is in some way privileged and owed special treatment or recognition…. When corporate authority does not recognize an individual’s inflated sense of entitlement, the criminal insider seeks revenge via electronic criminal aggressions.”

Dr Jerrold M. Post wrote Chapter 13 of the CSH5, “The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns.” He agrees that many criminal hackers who are employees (insiders) show signs of personality disorders. In particular, he warns that several types of insiders who have a past history of criminal hacking may engage in dangerous hacking such as inserting logic bombs for extortion, theft of information for industrial espionage, and development of a sense of ownership over the entire system for which they have been hired as system administrators.[p 13.7]

Dr Post has a list of recommendations for all IT hiring which are as follows:
The hiring process for employees in sensitive positions should be redesigned.

Monitoring, detection, and management should be improved.

Clear information technology policies should be formulated and briefed to incoming employees. An employee cannot be found in violation of a procedure if it is not clearly formulated and communicated.

Specialized support services for IT employees should be established. For example, IT employees are often reluctant to meet with an Employee Assistance Program (EAP) counselor but may avail themselves of online support services.

Screening and selection procedures should be augmented, to include online behavior by searching the Web using search engines.

Termination procedures are formalized.

Management of CITIs[computer information technology insiders] must be strengthened.

Enforce computer ethics policies and mandated practices.

Incorporate innovative approaches to the management of at-risk IT personnel.

Add human factors to computer security audit.

I recommend the following precautionary measures to be added to the usual hiring scrutiny when a candidate has revealed a questionable (criminal or borderline) hacking past (or present) or been discovered through a background check to have been or be involved in such hacking:

- Challenge the candidate openly and directly during an early interview about their actions; watch and listen carefully to evaluate the degree of honesty and insight with which the candidate discusses his or her past behavior.
- Ask the candidate to analyze a specific instance (which you select for discussion) of their past behavior from an ethical perspective; evaluate their depth of understanding of the ethical issues and of the ethical-reasoning process.
- Pose a hypothetical case involving a technically gifted employee who is badly treated by a supervisor and comes to feel abused. Ask the candidate to describe how such an employee might feel and what actions the employee might use to act on his or her resentments. Evaluate whether the candidate sympathizes with or approves of retaliatory behavior (you are looking for a sense of entitlement).
- Describe a case of criminal hacking in which someone’s personally identifiable information is stolen and used for identity theft. Ask the candidate to describe how the victim might feel. Look for signs of empathy (or its absence).

I think it is useful to test these questions on a couple of willing volunteers of known probity and long, loyal service among your technically-gifted employees to establish a baseline of responses from honest people and also for practice in asking the questions.

So before you hire a hacker, verify, then trust, then verify.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each
day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” (July 18-23)<http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php> “Management of IA,” (Aug 1-6)<http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php> and “Cyberlaw for IA Professionals.” (Aug 8-13)<http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php> Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

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 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.