Hiring Hackers: A Rebuttal (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Reader (and Norwich University MSIA graduate) Paul O’Neil disagrees with my suggestions in the recent article “Hiring Hackers”<http://www.networkworld.com/newsletters/sec/2009/081009sec2.html> published in this column. He has written a thoughtful and constructive rebuttal which has made me think critically about my position even though I disagree with him; I hope his two-part analysis will stimulate further discussion. Everything that follows in this second of two parts is Mr O’Neil’s work with minor edits.

* * *

The original articles on hiring hackers and criminal hackers into IT groups as programmers, network administrators and security personnel did not discuss the merits or the consideration of hiring a *bona fide* hacker. Many security professionals today portray infamous characters in the computer security world with a criminal history as miscreants such as Kevin Mitnick.<http://www.takedown.com/bio/mitnick.html> Yet I contend that Mitnick has done more to advance the world of computer security than thousands of security professionals.

I argue that we may be missing an opportunity to help advance the field of computer security even further by not including some elements of the hacker culture. Instead of closing the door on individuals that survived or profited in it, or achieved success however it is measured, we should try to leverage those hacking skills and consider improving technical security including all individuals in the discussion. Addiction psychology is employed heavily by former addicts in the field of psychology because they tend to make for better addiction specialists. Ostracizing all criminal hackers or potential hackers as misanthropes or worse with unjustified claims of a mental disorder demonizes people who could be contributors to our field.

Before Kevin Mitnick there was Frank Abagnale,<http://www.spiritus-temporis.com/frank-abagnale/biography.html> probably more successful at social engineering techniques than Mitnick, and even more technically advanced. Yet he was hired by the FBI to help combat banking crimes.<http://www.trutv.com/library/crime/criminal_mind/scams/frank_abagnale/index.html> If some hacker types are in fact motivated by notoriety or bravado, then we should harness that energy and turn what is generally regarded by security professionals as a negative into a positive. Let reformed hackers brag about defeating unreformed hackers.

In my opinion, current methods of computer security management support the increase of computer crimes. Slow-moving management structures are too slow to respond to evolving threats. Making it worse by depending solely on certified security professionals with the highest of ethical standards is not enough to defend a company’s information assets. Although it is hard
to measure security effectiveness when so many crimes go unreported (or worse, undetected), *bona fide* hackers seem to be among the few participants in the security field who do have measurable results.

Attempts to apply mental health diagnoses to potential employees unjustly stereotypes individuals by slapping a stigma similar to schizophrenia or criminal behavior with high recidivism rates in the absence of evidence.

Let’s not be dominated by the interests and motivations of the professional hacker when we are evaluating the potential of people involved in the hacker culture; motivations can change. And isn’t it usually through abuse of authorized access that some of the most devastating breaches are made? As Jerrold Post suggests in Chapter 13 of the *Computer Security Handbook, Fifth Edition, [http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/](http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/)* the bizarre situation in many organizations is that we impose fewer restrictions on casual workers than we do on our loyal long-term employees: “There is an interesting paradox that the less loyalty expected from a class of workers, the less attention is paid to their security threats. Thus, fairly careful screening, including criminal background checks and credit checks, is usually obtained for staff employees” – but we allow unbonded maintenance personnel from commercial cleaning companies to have complete access to our facilities.

Casual application of psychological theory in the absence of sound research methodology is no way to strengthen security. We should fairly consider former hackers as legitimate and valuable resources in the battle against computer crime.

* * *

Paul O’Neil, CISSP, is currently working as a Web programmer and security consultant. He has a Master of Science in General Psychology and a Master of Science in Information Assurance. He invites comment <mailto:paul@codeologic.net> on these articles.

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 Paul O’Neil & 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.