Hiring Hackers: A Rebuttal (1)

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 two-part 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 is Mr O’Neil’s work with minor edits.

* * *

Computer security researchers have published articles such as Chapter 12 of the Bosworth, Kabay & Whyne’s Computer Security Handbook, Fifth Edition<http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/> (“The Psychology of Computer Criminals” by Dr. Q. Campbell and David M. Kennedy) and Chapter 13 (“The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns” by Dr. Jerrold M. Post). These researchers correctly describe the nature of specific personality disorders, but their utility is doubtful in the context of computer criminals and computer crime.

It is still unclear how the science of psychology should be applied to the field of information security, especially when that science is incorrectly applied.

M. E. Kabay suggests in his second article on “Hiring Hackers”<http://www.networkworld.com/newsletters/sec/2009/081709sec1.html> that it would be useful to compose a questionnaire to use during the hiring process to filter for potentially dangerous hackers. He suggests, “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.”

“A couple of volunteers” to establish a baseline? That’s an awful baseline as the basis for inferring a Narcissistic Personality Disorder (NPD) in a potential new hire! And in general, pushing IA practitioners to apply psychological concepts to information security is risky: IA practitioners normally have neither the training nor the academic foundation in the field of psychology that would justify putting superficially-grasped concepts into practice. Applied psychology typically requires years of training to master.

I find it incredible to find NPD used in discussing possible personality disorders in criminal hackers (a term which warrants extensive discussion and definition in itself); NPD affects less than 1% of the general population. And to satisfy a clinical diagnosis of NPD, the Diagnostic and Statistical Manual of the American Psychiatric Association < requires at least five of the known criteria. In contrast, the computer researchers enumerate and repeat only two or three of the characteristics and ignore any differential diagnosis for other possible characterization.

Are the researchers implying that organizations should profile applicants to identify persons with
narcissistic tendencies or other personality traits that could indicate a vulnerability to a stress? Jerrold Post states in Chapter 13 of the CSH5, “The fact that individuals have many or even all of these personality traits does not mean that they will commit computer crimes. Rather they are particularly vulnerable.” It is here that I suspect Post borrows from the diathesis-stress model theory <http://en.wikipedia.org/wiki/Diathesis–stress_model>. And what is to be suggested from this? Are we to assume that we will not hire certain people because we think they may be predisposed to a mental disorder? Or is this approach misusing a legitimate psychological theory and misapplying it in the context of computer security?

Post continues, “It is often assumed that major computer crime occurs when there is an interaction between a vulnerable employee and stress... careful review of case studies of computer crime reveals a much more gradual time course.” Yet people who are considered clinically narcissistic would react swiftly and intensely when praise or expected reward are not forthcoming. Post writes that “individuals undergoing both personal and professional stress at the same time are particularly vulnerable” and goes on to describe how an IT specialist at a natural gas plant became distressed and “took the company hostage” by controlling the automated system in such a way it was a “bomb waiting to explode.” Isn’t this more comparable to a case of workplace violence? We should be analyzing such cases in the context of workplace violence rather than focusing on personality disorders.

Managing the risk of hiring a criminal hacker – someone convicted of computer crimes – can be handled using good old-fashioned background-screening techniques to discriminate among candidates and avoid hiring criminals. Instead, Kabay and others suggestion that organizations should profile individuals looking for telltale signs of potential criminal behavior. Observing narcissistic characteristics would raise a red flag for employers regarding a potential employee or even a current employee. But how accurate and beneficial is such categorization? Within the employee population of a typical medium to large organization, the chances are far greater that pedophiles, gamblers, drug abusers and so on are already employed – and these people pose a far greater risk to the organization than narcissists with a computer-hacking background. So while resources are diverted in a modern day witch-hunt for criminal hackers – or potentially criminal hackers – a loan broker masterminds a check-kiting operation that goes unnoticed until he is arrested.<http://www.mortgagefraudblog.com/index.php/weblog/comments/5328/>

Today, too many security professionals have received only boot camp training for a certification that supposedly qualifies them for positions of responsibility in computer and information security. However, I believe that without commensurate technical security knowledge and training, the situation is putting someone who has just completed drivers’ education training into a car at the Talladega Superspeedway. Adding pop psychology to information assurance practitioners’ background enhances their ability to defend computer networks less than it brings the undue stigma of psychopathology on other human beings.

In part two of this two-part series, Paul O’Neil analyzes the potentially positive role that reformed criminal hackers can play in information assurance.

***

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@codelogic.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.