Kevin Mitnick: How His Story Affected Information Technology, Security and Ethics

Robert Olson

The College of St. Scholastica

Abstract

Kevin Mitnick was one of the first people to hack into computer systems thus forcing information technology to create new security rules and regulations. How Kevin Mitnick had a more lasting impression is on the ethics surrounding information technology. The story of Kevin Mitnick explains how these changes came about.

Keywords: Kevin Mitnick, information technology, security, ethics

Kevin Mitnick: How His Story Affected Information Technology, Security and Ethics

Kevin Mitnick could have been my friend except for the facts that he is slightly older than I am, grew up in California, and was interested in breaking the law. Mitnick started out as a phone phreak, or someone who could take over a telephone company's digital central office and play pranks through the phone. He was first arrested in 1981 for breaking into Pacific Bell Telephone Company and stealing technical manuals. He then moved up to breaking into a Pentagon computer and the military's NORAD air-defense computers and spent his first stint in jail for six months in a juvenile prison in 1983. In 1989, he illegally downloaded source code from Digital Equipment Corporation and this is where rumors started saying that he was capable of launching nuclear missiles simply by whistling into a telephone. Because of the fear of his power, he spent one year in federal custody, eight months of which were in solitary confinement so he could not have the opportunity to whistle into a phone. After being released, he also spent six months in a halfway house for his addiction. He was to then have three years of supervised release, but he violated this probation and went underground in 1992. (Freeman et al., 2008)

During the next three years, Mitnick broke into many large companies' computer security systems and stole software, product plans, and other data. These companies included Motorola, Sun Microsystems, Nokia, and Novell. According to prosecutors, these cost the companies $80 million in damages. He was listed on the FBI's most wanted list. Finally on February 15, 1995, he was captured at his hideout in Raleigh, North Carolina. He was held without bail for five years and again spent eight months in solitary confinement. He was not allowed to use a radio, telephone or even the electric typewriter in the prison library. In March 1999, Mitnick pleaded guilty to wire and computer fraud costing he feels $5 to $10 million in damages. He was sentenced to another ten months in prison and had to pay $4000 in restitution. He was released on January 21, 2000, and was on parole for three years during which he was not allowed to even touch a computer, use a cellular or cordless telephone without permission from his probation officer, or write, speak or profit from his experiences. These terms have since been relaxed so he can write, lecture, and consult. (Freeman et al., 2008; Huang & Wu, 2005)

This sordid tale has inspired the movie *War Games,* and Mitnick is the subject in the movie *Takedown.* Three books have also been written including *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw By the Man Who Did It* by Tsutomo Shimomura and John Markoff, *The Fugitive Game* by Jonathan Littman, and *The Art of Deception: Controlling the Human Element of Security* by Kevin Mitnick himself. Mitnick has also made a guest appearance on the TV show *Alias* and was interviewed on *Sixty Minutes.* (Accadi, 2002; Flynn, 2002; Freeman et al., 2008; Meyer, 1995)

This all begs the questions as to what does Kevin Mitnick have to do with IT security and ethics, why was everyone enamored with his story, and would you want him to work for you? First, Mitnick in his own words says, "Hacking is a skill set – how you use it is up to your ethics and morals" (Huang & Wu, 2005, p. 21). Mitnick used his abilities to the detriment of society and was punished for that; he now is using his abilities to help against hackers.

Next, why was Mitnick so popular? No one disagrees with the fact that he was very good at what he did and he was breaking the law meaning that he was breaking and entering and stealing. That being said, hacking is a different kind of crime in that what is being broken into is not a physical place and what is being stolen still exists at the place from which it was taken thus leaving an air of ambiguity as to what was actually stolen and how or if it is being used. According to Meyer (1995), Mitnick claims that he hacked to gain information and power rather than for money and malice. Does this make the crime any less? Did Mitnick receive an unusually harsh punishment due to the hype that surrounded his alleged abilities? In one article, it says that people are fascinated with the Robin Hood type drama "…as long as no one is injured, there is an element of cleverness and originality in the crime, and the victims are wealthy individuals, pompous politicians or large, impersonal corporations" (Freeman et al., 2008, p. 5). This describes Mitnick and his hacking activities to a tea and explains his notoriety.

Finally, Mitnick is currently a highly sought after consultant for companies and governments where he tests their security systems. Hacking is still a very common crime. One test Mitnick conducted in 2009 recorded 1,300 attacks per hour on machines without an active firewall. He believes that "Computer systems are complex. There will always be ways to break in" leaving the authors Huang and Wu to comment, "Which means that no matter which side he is on – let's hope it's ours – Mitnick will always be in demand" (2005, p. 21). Would I want to hire him as a security consultant for my company? I am of two minds on this. While I believe his skills would be useful, I am not sure that I trust his new found morality. Letting him in to know the secrets of my company would require a level of confidence that might be too high. That being said, I believe he could break into my company anyway if he wanted to so that issue is moot. Hiring someone like Kevin Mitnick, who knows the backdoors, would be helpful to point the loopholes in the security system. Hopefully he will continue to use his skills to aid in the fight against hackers and support security systems to the betterment of society.

References

Accadi, J. (2002). The art of deception (book). *Library Journal, 127*(13), 128. doi:10/789651sdf1898156575657

Flynn, M. K. (2002). It takes a hacker. *PC Magazine, 21*(18), 26. Retrieved from www.pcmag.com/

Freeman, E. H., Johnson, R., Anderson, P. Q., Smith, E., Quele, I. G., Reele, B., … Yellow, O. (2008). The legend and legacy of Kevin Mitnick. *Information Systems Security, 10*(2), 5-9. doi:98129872621//droks21981

Huang, G. T., & Wu, A. (2005). The talented Mr. Mitnick. *Technology Review, 108*(3), 21. doi:107832/fds12699512

Meyer, M. (1995). Is this hacker evil or merely misunderstood? *Newsweek, 126*(23), 60. Retrieved from www.newsweek.com/