The psychology of the cybercriminal

Dr Iain McCormick
Executive Coaching Centre

Research produced in 2016 by the threat intelligence experts, BAE Systems[i] has identified the six different cybercriminal types that represent the biggest threats to Australian and New Zealand businesses. Their research report called *The Unusual Suspects* is based on extensive analysis of thousands of cyber-attacks on businesses and identifies the most common types of cybercriminal. The company report details six cybercriminals:

- **The Professional** – career criminals who 'work' 9-5 in the digital shadows
- **The Insider** – disillusioned, blackmailed or even over-helpful employees operating from within the walls of their own company
- **The Mule** – naive opportunists that may not even realise they work for criminal gangs to launder money
- **The Nation State Actor** – individuals who work directly or indirectly for their government to steal sensitive information and disrupt enemies' capabilities
- **The Activist** – motivated to change the world via questionable means
- **The Getaway** – the youthful teenager who can escape a custodial sentence due to their age.

If these are the types of cybercriminals, what drives them and what is the nature of their personality. Regrettably there is very little sound psychological research in this area. An early report on self-reported computer criminal behaviour[ii] studied seventy-seven students enrolled in an information technology programme who participated in the web-based study. The researchers examined students' personality, types of moral choice made and the degree of manipulative exploitative behaviour of the students. The results of the study indicated that the only significant variable for predicting criminal/deviant computer behavior was introversion. Those individuals self-reporting criminal computer behaviour were significantly more introverted than those reporting no criminal/deviant computer behavior. As a very large slice of the population are introverted this study tells us very little!

A recent study from the International Journal of Cyber Behavior, Psychology and Learning[iii] investigated the relationship between personality, coping style and cyber-bullying experiences. This study used 300 Greek pre-adolescent students at primary school. Boys reported more frequent involvement in cyber-bullying incidents, while there were no significant gender differences in terms of cyber-victimisation. Their analyses indicated that boys with a lower work ethic who use passive avoidance were more likely to cyber-bully.

An interesting conference paper by Dinei Florencio from Microsoft suggests that much of the information on cyber-crime is gathered from unreliable surveys[iv]. Again reinforcing the idea that actually we know very little about the nature of cyber-criminals.

If you want to find out more you may be interested in a seminar session with Kevin Mitnick, who used to be the FBI's "Most Wanted Hacker". The seminar will be held in Auckland on 22 August. During the seminar, Kevin Mitnick will demonstrate in a live hack session the latest hacking techniques, highlight the vulnerability of organisations and offer solutions based on his experience as a hacker and the CEO of a highly successful cyber security consulting firm. See http://www.mitnicklive.com

---

i https://itbrief.com.au/story/unmasking-cyber-criminals-research-unveils-six-cybercriminal-personalities/

ii Marcus K. Rogers, Kathryn Seigfried, Kirti Tidke, Digital Investigation 3S (2006) S116–S120

iii http://s3.amazonaws.com/academia.edu.documents/33216163/Cyber-Bullying-Personality-and-Coping-among-Pre-Adolescents.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1469922566&Signature=k%2FF6OOvxR2fCG4LsMqZS7r6Od34%3D&response-content-disposition=inline%3B%20filename%3DCyber-Bullying_Personality_and_Coping_am.pdf

iv https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SexLiesAndCyberCrimeSurveys_ITTC.pdf