Information Security Now – 48

Ethics v Morality in IT

John Mitchell

As an IT assurance provider I am governed by the codes of conduct of four professional associations, plus those of the industries that I work within and the statutory and regulatory frameworks of the different countries I visit during the course of my work. Surely I have sufficient guidance to operate in both an ethical and moral manner? However, there is a clash between ethics and morals. Both relate to "right" and "wrong" conduct and while they are often used interchangeably, they are different. Ethics refer to rules provided by an external source, e.g., codes of conduct, while morals refer to an individual's own principles regarding right and wrong. If you are reading this as a member of the BCS, of whatever grade, you are bound by the Institute's code of conduct. A part of this requires you to have due regard for public health, privacy, security and the wellbeing of others and the environment.

When James Liang of VW diesel gate fame, created a software routine within the engine management system of some diesel cars, which lowered exhaust emissions when it detected that the vehicle was running on a test rig rather than on the road, he committed a criminal offence by breaching US clean air legislation. As a result he received a forty month prison sentence and a large fine. He would also, had he been a member of our Institute, breached our code of conduct. Unfortunately, only a minority of IT people are members of any professional association, so they tend to operate within a framework of societal ethics and their own morality. Liang may have been simply following orders from above, but this was ruled as not being a defence as long ago as the Nuremberg war crimes trials between 1945 to 1949. However, where does this leave others involved in our profession? If I program a nuclear missile guidance system in the full knowledge that the end result is the likely death of millions of people, then surely I have breached our code of conduct regarding the wellbeing of others? What if I knowingly program a driverless car to kill one person as the cost of saving five others, or write software which will cut-off the energy supply to one street in order to keep a town supplied? The permutations are almost limitless, but the clash between ethics and morality is something that we seldom think about. Indeed, is there a clear right, or wrong answer to the moral maze in the scenarios I have outlined?

The contradiction between ethics and morals in IT is no-where more clearly illustrated than in the concept of white-hat hacking. The law may state that unauthorised access and/or modification is a crime, but if one's intention is to notify the company of a vulnerability in order to have it fixed, then is such action morally defensible even though it is ethically wrong? Some companies have 'wised-up' to the need to have their systems tested with any vulnerabilities notified to them, rather than used against them. Facebook received 12,000 submissions from hackers (now redefined as researchers) in 2017, paying out a total of $880,000. It has paid out a total of $6.3m since it started its programme in 2011. Google has paid out $12m in rewards since 2010, paying $2.7m in

2017. Its biggest reward in 2017 was $112,500 to someone who detected a security flaw in its Pixel smartphone. Following the recent Spectre and Meltdown bugs in its chips, Intel too has upped its top rewards to $250,000.

So, there is real money to be made from ethical hacking. According to figures from *HackerOne* the top hackers in India earn 16 times the median salary of a software engineer. On average, top earning ethical hackers make almost three times the median salary of a software engineer in their home country. Apple only launched its bug bounty programme in 2016, but so valuable are bugs in its software, with several secretive companies offering up to $1.5m for a high-level attack flaw, that some in the ethical hacking community have suggested that Apple's own payments, which range from $25,000 to $200,000 are simply not large enough to prevent hackers moving to the dark-side. Money talks and if the bad guys are willing to pay more than the good guys, then it is likely that the moral compass will swing to them.

The Institute's strap line is 'making IT good for society'. However, the 'good' is open to interpretation. Returning to my nuclear missile guidance system analogy, it could be argued that rather than doing potential harm to society I am actually doing good, by preventing an attack which could kill millions through the mutually assured destruction paradigm. However, this assumes that my system will never be used for a first strike. No such defence is available to James Liang whose actions may well have incurred the death of thousands of people through air pollution. His was a clear attempt to circumnavigate societal safeguards. Due to the general lack of board oversight of IT, coupled with their lack of technical knowledge (the digital deficit), it is not too surprising that IT professionals are given a great deal of autonomy in what they produce and deliver. IT staff do not generally receive education in governance and seldom in ethics, or morality. Being a part-time academic, I am well aware of the paucity of these subjects in the undergraduate curriculum, which tends to concentrate on delivery and speed of response as against is this the right thing to do? This is similar to the situation in the accounting profession some fifteen years ago when there was very little training in these areas. Indeed, Jeff Skilling, the Enron[1] CEO, famously boasted that he had never attended a single seminar on ethics when at Harvard Business School. My niece 'wrote' a system of some ten thousand lines of underlying code simply by painting the screen with what she required. The result was a joy to look at, but contained little in the way of controls and I was able to crash it simply by inputting alphas into a numeric field. Not a kindly uncle thing to do, but it illustrates the need for the academic world to teach governance, control, and assurance alongside the technical aspects. Seasoned hackers love the challenge of breaking a system, but if the system has been produced by trusting people such as my niece, using off-the-shelve tools, it is not really a fair fight. We should also be cognisant that the motivation of hackers may not be financial gain, but something else which chimes with their own morality construct.

Writing this article has made me realise that our strap line is open to wide ethical and moral interpretation, especially the word 'good'. Also, if the white-hats are hacking systems for financial reward is that morally justifiable? I am

[1] Subject of a big accounting fraud in 2001

sure that I can argue the case either way and, for the record, I received no financial compensation for this article.

John was recently awarded the John Ivinson medal for services to the Institute. He is a previous member of Council and the Risk, Audit and Finance Committee. He is currently Treasurer of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638