Ryan A Davis

CSE 488

2 February 2012

Data Theft and Corporations: An Ethical Analysis

What happens when employees steal vital data from within their own company? And what are the justifications for such acts? Data theft or "Cyber-mole" crime, a steadily increasing Information Security issue, is becoming a significant financial problem for global businesses and corporations. Cyber-mafia gangs armed with malicious software utilize "phishing" and "whaling" techniques to deceive corporate employees into providing account passwords, which enables them to access the corporation's database. With data theft now being responsible for an estimated one trillion dollars, it is considered a new threat that could potentially cause a great economic meltdown for international organizations should they fail to actively prevent these malicious acts. Computer information security analysts suggest the increase of "in-house" cyber-crime and the vulnerability of vital company information is due to the current dire economic conditions and cites shrinking paychecks as the primary motive for such actions. Despite this, there is no way to justify the actions of these cyber-moles and data hackers. The theft of intellectual property is morally and ethically wrong, in any event, for any reason.

The reasons as to why stealing digital data is morally and ethically wrong are vast. The financial repercussion in itself would be colossal, and has the potential to not only destroy a company and cause thousands of workers to lose their jobs, but could also

cause an economic meltdown on a global scale. If a data breach occurred at a particular business, physical harm could also ensue. If someone lost his job due to a corporation shutting down resulting from a data breach, he could enter a state of massive depression and develop various psychological problems, and even contemplate suicide. If a major data-breach occurred at a medical organization or hospital, it could drive day-to-day operations into a state of absolute chaos. And furthermore, we should assume that lives would be lost as a result of misdiagnosis or medical professionals being unable to do their duty, due to an absence of much-needed data resources such as patient information.

It is fairly obvious that the cyber-moles and hackers primarily employ the mentality of egoism to justify their actions, seeing as the only persons who benefit are the data-hackers themselves, and offers nothing but harmful after effects to the other parties involved. When carrying out the action of entering a computer system and retrieving important data for the sole purpose of stealing it, they are doing so under the assumption that they'll make a financial gain. This course of action, with the hacker being directly aware of the consequences, meets the definition of egoism. We should assume there exist malicious parties who are aware of simple ethical standards, policies, or rules that deem it inappropriate to commit theft of intellectual property from an organization.

We could also include other forms of ethical systems to justify the actions of the data-hackers. Situational ethics, which describes how the morality of an act is determined by the state of a system, can also be applied to this situation. The cyber-moles could justify their actions by suggesting the circumstances under which an organization is operated is simply asking to be taken advantage of. Considering the rapid

expansion of digital data is becoming much more important every year, the state of the industry-wide standards leaves policy vacuums and gaping holes that allow users to enter a system in which they are not allowed permission. Perhaps hackers believe that the computer data systems with less security are inexcusably vulnerable, or the high-powered associates who fall victim to phishing scams should know better, and deserve the consequences that follow. A group that has exhibited this type of behavior is the recent "Hacktivist" group Anonymous, who breached US government websites and Sony's Playstation 3 network. Anonymous did nothing with the data attained, but rather did so in an attempt to clearly point out how vulnerable the systems were, and how easy it was for them to infiltrate the computer systems of the worlds largest organizations.

A high majority of outside hacking comes from obscure areas of the world, and leads us to consider a form of Nihilism to explain their actions. Cultural differences, societal norms, and a lack of authority are all valid reasons to assume hackers disregard basic computer ethical standards. For example, in November 2011, Russian cyber-criminals hacked into an SCADA software infrastructure control system in Springfield, Illinois and took over its water facility. They then proceeded to turn the pumps on and off repeatedly and broke the main water pump, causing major damage and financial loss. The hackers were traced to a remote part of Russia, and it is assumed that due to the isolation from society, they are likely far removed from any set of particular cultural standards and have a disregard for authority. Russia, along with Pakistan, China and other Asian countries are considered "hot zones" for hacking activity, due to various economic and cultural reasons.

The behavior of these cyber-moles and hackers is not consistent with either the IEEE code of ethics or the ACM (Association for Computing Machinery). The malicious actions outlined in the news story are dishonest, harmful to others, do not honor property rights or privacy, and exhibit a blatant disregard for data confidentiality, all of which are direct violations of the ACM and the IEEE code of ethics. The fact is, the consequences that would result from the malicious activity would directly endanger the welfare of the public, an infringement upon the very first code in the IEEE code of ethics. The hackers also break the ninth IEEE code as well (which states that one shall not hurt others, their reputation, or employment by false or malicious activities), which was violated during the data breach we are analyzing. According to the study, international organizations have lost an estimated one trillion dollars, and there is no question that many people were harmed and the reputations of the organizations greatly effected.

Perhaps there is a valid justification as to why the cyber-moles and hackers are performing these malicious activities. The egoist mentality can be a result of needing the money (from selling the vital corporate data) to feed their family, or to pay medical bills for an ailing family member. We should assume some of the cyber-criminals are possibly forced to a certain point where they absolutely and desperately need the money for such reasons, which would justify the needs of an egoist. They want what is good for them at the expense of others.

Also, Nihilists, perhaps unhappy with what they define as unequal business standards or levels within an organization, can justify their actions by believing they are leveling the playing field when forcing these companies to pay billions of dollars in data

recovery services. In fact, both the cyber-moles and outside hackers display an obvious contempt for all levels of authority and morality, as the outside hackers don't appear to be concerned with any government or law enforcement agency, and the inside cyber-moles exhibit the behavior of someone who has no moral boundaries when stealing critical digital information and causing substantial financial damage.

Regardless of what ethical systems we analyze in order to excuse these actions, there are no justifications that can validate them. Stealing, in any case, is morally and ethically wrong, whether it's money, property, or intellectual property. The theft of property is an act that transcends all boundaries of morality, cultures, and religious faiths. Regardless of where one comes from, socio-economic level, the cultural standards by which you're born into, stealing from another party is never morally nor ethically justified. There are other means by which the hackers could've attained money, by either simply working harder or getting another source of legitimate income. The mindsets of the hackers were not ethically moral (i.e. Utilitarian), and were mostly self-centered and with a great disregard for authority, which doesn't meet the standard of nearly all codes of ethical standards.

The growing importance of digital data and intellectual property is becoming increasingly apparent, and with the loss of said property could yield severe economic consequences on a global level. New technology introduces new standards, and new ways to look at ethics as they relate to rapidly changing technology. This case is a great example on how, as computer professionals, we should protect the integrity of digital data and withhold the ethical standards in an organization. By increasing security of the

user-permission rights amongst computer users within an organization, we can set maintainable parameters and better control the access-level of particular levels of data. However, while forging ahead in security management, we must always analyze the ethical structures in which these systems operate.

Works Cited

Smith, Graham. "Hackers Take Control of U.S. Public Water Treatment Facilities | Mail Online." Home | Mail Online. DailyMail, 21 Nov. 2011. Web. 05 Feb. 2012. http://www.dailymail.co.uk/sciencetech/article-2064283/Hackers-control-U-S-public-water-treatment-facilities.html

Pratt, Alan. "Nihilism [Internet Encyclopedia of Philosophy]." Internet Encyclopedia of Philosophy. Internet Encyclopedia of Philosophy, 23 Apr. 2001. Web. 05 Feb. 2012. http://www.iep.utm.edu/nihilism/

ACM Council. "ACM Code of Ethics and Professional Conduct— Association for Computing Machinery." Association for Computing Machinery. ACM, 16 Oct. 1992. Web. 05 Feb. 2012. http://www.acm.org/about/code-of-ethics

IEEE. "IEEE - IEEE Code of Ethics." IEEE - The World's Largest Professional Association for the Advancement of Technology. IEEE, 1 Feb. 2010. Web. 05 Feb. 2012. http://www.ieee.org/about/corporate/governance/p7-8.html

Lander Education. "Ethical Egoism." Philosophy Home Page. Philosophy Lander, 26 June 2011. Web. 05 Feb. 2012. http://philosophy.lander.edu/ethics/ethical_ego.html