Ethical Computing for Data Protection

Wanbil W. Lee, Wanbil and Associates, Hong Kong & Computer Ethics Society, Hong Kong

ABSTRACT

Data protection is a chronic problem. Technology has had a social and ethical impact on our professional, social, and private lives. It is imperative for computing practitioners and researchers to link the ethical dilemmas and the technologies to the relevant ethical theories. This paper argues that the cause is rooted in our indifference to ethics—one doesn't take ethics as seriously into consideration as one should when formulating information security policies and protection standards—and proposes an ethics-based approach that can lessen the incidence of hacking or make hacking exasperate, aiming at mitigation rather than eradication. Central to this approach is ethical computing preconditioned on a sound understanding of the applicable theories of ethics and a shift of view of risk and ethics.

KEYWORDS

Computer Ethics, Cyberattack, Cyberwar, Data Protection, Ethical Analysis, Ethical Computing, Ethical Matrix, Ethical Risk, Hexa-Dimension Metric

INTRODUCTION

Data protection is a chronic problem, a nightmare that haunts information security and corporate management perennially. The symptom is the incidence of cyberattacks continues and the cost of damages keeps on soaring despite the big spending on cybersecurity up to billions of US dollars (Firstpost, 2018; Gartner, 2018; Talevski, 2018) yet data protection must go on despite a disappointing return of investment on countermeasures. While the cause is arguably rooted in our indifference to ethics – we do not take ethics seriously into consideration as we should when formulating information security policies and protection standards, the diagnosis is a lack of a sound understanding of the applicable theories of ethics and a shift of view of risk and ethics (Lee, 2018a). This problem needs urgently a remedial action, an ethics-based approach that aims to mitigate rather than eradicate, that is, to lessen the incidence of hacking or make hacking exasperate, due to the vicious circle effect (Lee, 2015a). To apply the proposed remedial framework is preconditioned on a good appreciation of the social and ethical impact on our professional, social, and private lives consequential upon the advance of the technologies (Stahl, Timmermans and Mitttelstadt, 2016), in order to link the ethical dilemmas and the technologies to the relevant ethical theories. This paper will demonstrate the remedial framework successively through a description of its key components including the main tools: Ethical Matrix and Hexa-dimension Metric and concludes with an illustration of linking theories to situations using a few cases.

DOI: 10.4018/IJT.2020010104

THE SYMPTOMS

Spending on Security

Security budges rise exponentially and amount to millions of dollars. US Homeland Security Research reported that major financial institutions spent in 2016 US$1.5 billion on cybersecurity (US Homeland Security Research, 2016). PWC reported that UK organizations doubled spending on information security: on average £6.2m in 2016 compared to £3m in 2015 (CyLon, 2017). Gartner predicted worldwide spending on information security would reach $86.4 billion in 2017, and expected it to grow to $93 billion in 2018 (Bradley, 2017). Further, Gartner indicated that Hong Kong was to reach HK$3.5 billion this year, that mainland China to reach almost 23.9 billion yuan (HK$27.2 billion) and 27.3 billion yuan, respectively this year and in 2019, and that global spending to reach more than US$114 billion this year and to US$124 billion in 2019 (Bushell-Embling, 2018).

Ramifications of Cyberattacks

Cyberattacks culminate in conflicts at different levels and scales, ranging from individual victimization to nation-to-nation wars. The term, cyberwar, was initially coined for symbolizing conflicts between hackers from one country and targeted firms of another country (such as espionage campaigns) resulting in the theft of business information such as bid prices, contracts and information related to mergers and acquisition, for example, the US-China trade-based and military-oriented cyberespionage some years ago (Onag, 2018). The alleged Russian interference of the US general election in 2016 (The New York Times, 2018a) and the battle between UK and Russia over the tampering of Brexit voting (The New York Times, 2018b) are other examples of cyberwar.

Cyberwar is gradually used to denote conflicts at lower scales, between business organizations, interest-groups, etc. For example, "Blocking of Internet Advertising" is a battle between advertisers and users ad blockers (Wicker and Karlsson, 2017). The following three cases of cyber-ransom exemplify another type of cyberwar. First, WannaCry has hit computers from the UK's National Health Service and infected dozens of computers every minute in mid-2017. Second, WannaMine took over computers around the world, hijacking them to mine a cryptocurrency called Monero early this year (The Telegraph, 2017). Third, a ransomware encrypted the files of infected users, and demanded payment for decryption of US$300 (HK$2,300) in bitcoins within three days, US$600 (HK$4,700) after the three-day deadline, and all the files would be permanently encrypted after one week (in Hong Kong on 15 May 2017) (Hong Kong Free Press, 2017).

THE CAUSE

Intuitively, we blame the extant "ammunitions", but it is not fair because the data protection software is implemented according to the design so the fault should lie in the design, not in the ammunitions themselves. Therefore, the extant software being impotent can only be secondary if it is a cause.

Then, again, the design itself should not be blamed because design is governed by the data protection policies (at corporate level) and standards (at operation level). Hence, the design, which leads to unsatisfactory results. These policies and standards are silent on the socio-ethical aspect of the problem but concentrate on ensuring a good return on investment of the technology (financial viability) and an optimal utilization of technologies acquired (technical efficiency). It follows that the ammunitions, designed according to these policies, are incapable of covering issues of a social/ethical nature. By implication, the fault lies in the policies and standards, another higher-level cause. By deduction, the primary cause is that we do not take ethics seriously.