English
Research Express@NCKU Volume 10 Issue 6 - September 11, 2009
[http://research.ncku.edu.tw/re/commentary/e/20090911/1.html]

Weaving a Safety Net for E-shopping

Yung-nane Yang

Professor of Department of Political Science and
UDD Director & AVP for R&D, National Cheng Kung University

This article has been published in China Times on June 15th , 2009.

Yesterday the Eastern Home Shopping (EHS) was revealed to have leaked 8,000 credit card transaction data, inducing anxiety among the public because e-shopping is so popular nowadays. Many victims came to realize that their personal data have been cheaply sold to ruffians only after receiving defraud calls and being cheated. There might be more victims unaware of their personal data being exploited improperly by ruffians. The consequent problems such as fraud, kidnapping, blackmail and other improper use would result in social problems of inducing serious physical and mental harm to the victims. Hence one must ask: what are the reasons for serious leakage of personal data? Who should be responsible for this?

First of all, the businessmen who intend to enter e-shopping should invest in Internet security at the same time. They should not have been so irresponsible to have let the ruffians set up Trojan programs so easily to the e-shopping website and have exposed the customers' personal data in such an unsafe environment. Since the businessmen profit from e-shopping, it is their obligation to provide a clean and safe shopping environment. Just like regular stores, if they cannot provide a clean and safe shopping environment, they will be despised by the consumers. In other words, the businessmen should be held most responsible for leakage of personal data; the rationale is the same as companies should be responsible for flaws in their products. The businessmen should invest in hardware and software equipments and hire information and communication security staff and actively improve security and protection for personal data in e-shopping (there are few news stories of personal data leakage incidents with Internet banking and the reason for this is that the banks are conscious of the risks), otherwise similar incidents will pop up one after another.

Interestingly, the businessmen regard themselves as the victims, because they are unaware (of course there is a possibility that they know) the website is hacked by Trojan programs and personal data are hence transcribed. According to media report, there has been a regular occurrence in the long-term problem of EHS's personal data leakage. Apparently the businessmen lack the ability to learn the lessons, or, the author suspects they do lack the resolution (to be willing to spend on Internet security infrastructure) to solve the problem. Without government mandates and rules, I'm afraid not much could be achieved by encouraging consumers to boycott uncommitted businessmen. Hence, another issue in concern is: how can the government strengthen the management and regulation mechanism on immoral e-shopping companies?

To put it simply, the direct cause for the personal data leakage problem is insufficient government

inspection. But to dig beneath the surface, it is likely that there lacks an authority institution in charge of Internet security and leave the problem unsolved. Therefore, except for the businessmen, the government also is accountable for developing a well-functioning management and regulation mechanism. However, which department of the government is responsible? The Executive Yuan has organized an Information & Communication Security Technology Center (ICST); however, such cases might not be qualified to be listed in the ICST's agenda because they are not directly related to national security. Or, even if they are listed in the agenda of ICST (which is only a taskforce), the capacity to solve problems would be limited because the members might dump the responsibility to one another. In the end, it is necessary to hold an authority institution in charge, but which will that be?

In fact, to handle Internet personal data leakage incidents and Internet fraud crimes is the responsibility of (cyber-) police. However, the police is only responsible for the crimes, and the management of Internet information security is not one of their job duties. Hence, currently, the National Communications Commission (NCC) should be the authority institution in charge of e-shopping. However, it is likely that the NCC lacks legislations and practical experiences, resulting in the government's unsatisfactory performance on management of the companies. Currently, the government's rule and inspection imposed on business Internet security is nearly null, allowing similar incidents to occur continuously. It is definitely the government's duty to clarify the issue and establish a policy for management and regulation of personal data leakage in e-shopping. It will be the best for NCC, which is familiar with the affairs, to take initiative and propose legislation to let loose or an executable management plan, for this will be the truly proficient solution.

Moreover, if the police in charge of Internet information security related cases realizes the impact of the issues and understand the problems originate from NCC's management and regulation policy, they should have a mechanism to get the attention of their supposedly "superior" institution NCC. However, according the current operation model, there does not seem to have such a communication or collaboration mechanism, and this is where we (the government) should endeavor. Furthermore, if the Executive Yuan can work out a compensation mechanism (legislation) immediately, allowing the victims of personal data leakage to plea for compensation either from the business or the authority institution in charge, I believe both will take actions right away to insure security of the public's personal data.