

**Speech by Dr. Elizabeth Quat,  
President of Internet Professional Association at the  
HKIE IT Division Annual Conference  
CITPP 2006  
*Optimizing IT utility through efficient project management  
and ethical practice***

**Roundtable Discussion on  
*How effective is Computer Ethics a countermeasure  
against Computer Crime?***

4 May 2006, 16:50 – 17:50

Ladies and Gentlemen, Good Afternoon.

I would like to thank HKIE ITD for organizing this meaningful discussion and it is my honor to share with you some of my views about the subject.

1. Internet Professional Association and I believe that Computer Ethics is one of the most important factors, or measures against Computer Crime.
  
2. Due to the growing intrusion of the Information and Communication Technology (ICT) into all realms of everyday personal and professional life, the ubiquity of computers, and the quickly shared knowledge of their vulnerabilities, individuals, companies and organizations can and must assure their own protection. This is not merely of pragmatic concern, but a moral responsibility and ethical mandate due to the severe consequences to individuals, stockholders and customers, and to the general public as a whole, and moreover, due to the growing importance and reliance by societies upon computing systems.

ICT is considered both a tool to build and a weapon to do harm. It is a powerful tool to be used by people. And generally, we believe that people's decisions and behavior are mainly guided by their value.

3. Computer Ethics as a branch of professional ethics, is a Value about how computing professionals should make decisions regarding professional and social conduct.

But what is and is not ethical with regard to activities involving ICT?

- One popular view among hackers is:

“Breaking into a computer should not be a crime! No one get hurt and we all learn something.”

- “Forester” has a line about software development that reflects some ethical concern: “Another extraordinary aspect of software marketing is the fact that the user generally pays for software updates. In other words, even if the product is faulty or needs amendment, the user pays the software supplier to provide more correct versions.”

- While it is mandatory for Civil Engineer to have a license or at least registered to design and build bridges, roadways, buildings, transit systems, dams, etc... Software Engineers who Design and construct some of most life threatening system such as: Medical diagnostic equipment control and command system, Air Traffic Control Systems, Strategic nuclear weapon control systems, Software components of anti-aircraft/missile systems, Automotive computer control systems, Banking and Financial systems, and for Programmers who conduct the implementation of all the above mentioned systems do not required any license in Hong Kong.

- Due to their growing presence, computers will be increasingly used by organizations to defeat or undermine their adversaries, either real or perceived. Naturally, anyone using technology to defeat or injure his enemy will feel justified in their actions

The opportunity to make lots of money, having fun without concerning responsibilities, or cause great harm and remain anonymous heightens the need for individuals and organizations with computing resources to maintain a high ethical balance to their operations.

4. Some research findings believe that if people are made aware of the consequences of their actions that fewer people will be motivated to plant dangerous computer viruses, contaminate information systems with false information, or post pornographic material onto the Internet. That ethics-conscious people will be more likely to protect personal privacy, honor the copyright laws and report unethical activity.

If ethical abuses are left unabated, all roads on the information superhighway will be toll roads for encrypted data. If this were to happen, we would become a more secretive society, far less willing to share accumulated knowledge. Moreover, computer crimes may affect the development of our economy and national security.

5. Information security and computer ethics are also issues of current international concerns. It is clearly stated in the Tunis commitment document of the United Nations World Summit on the information society point no. 9 that “build capacity; increase confidence and security in the use of ICTs;... address the ethical dimensions of the Information Society; and encourage international and regional cooperation... are the key principles for building an inclusive Information Society.”

It is also stated in point 15 that: “ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals.”

6. Recent incidents involving leakage of personal data made the fact evident that organizations in Hong Kong are lack of computer security awareness and training, especially in setting up security measures when storing and transmitting personal data by electronic means.

When talking about professional ethics, just legally right should not be the ceiling of the standard. Besides legal, we should also consider reasonable and responsible.

As an ICT Business operator, I currently encountered client requested to add an unlimited liability clause in the contract to protect their data security. The action is a reflection of non IT organization’s lack of knowledge and guideline in handling data security, and the general public’s lack of confidence in the professional ethic of ICT practitioners. Without effective measures, this kind of request will become more popular, and sooner or later may jeopardize the development of Hong Kong ICT industry.

We believe an awareness and educational programme to raise ICT professionals’ awareness of computer security and personal data privacy and to encourage organizations to overhaul security measures in protecting customer information is needed.

We recommended that ICT Ethics and Governance be integrated into all college curricula, and in the future be included in primary and secondary schools as well. And the government should allocate more resources in public awareness and training. Besides education, in the long run, monitoring and regulation should also be included in our industry and government involvement. Therefore, other than a code of ethics, industry and government should also consider developing a legal binding code of practice.

7. iProA together with HKIE ITD, the Office of the Privacy Commissioner for Personal Data and other ICT Associations are committed to planning and implementing a series of actions including:

- Develop an Information Security Guideline for Corporation that holds personal data and for ICT professionals and practitioners

- Promote the guideline and conduct Information Security training and workshops for professionals, individual and SMEs

- Promote best practices in ICT Governance and latest technologies in information security

- Study to develop a Code of Practice for ICT professionals

The recent incidents of personal data leakage is definitely a tragedy but it also act as an alarm to the society and offer us a golden opportunity to work together to tackle the problem. There are a large number of unknowns when dealing with computer crime that need far more studies, discussions, and actions. We hope our recommendation and actions are just the starting point.

Thanks for listening.

- END -