Yui Kee Computing Ltd.

Newsletter

September 2010

Contents

Contents 1
Humour: xkcd on Password Reuse 1
First INTERPOL Information Security Conference 1
Malware: The Anti-Personnel Mine of Cyberwar 2

Humour: xkcd on Password Reuse

<web-link for this article>

The real purpose of online services...

Password Reuse

First INTERPOL Information Security Conference

<web-link for this article>

The first INTERPOL Information Security Conference took place from 15th to 17th September 2010 at the Hong Kong Police Headquarters with the theme of "Global Cooperation Today for InfoSec Risks Tomorrow", and brought together industry leaders, academic experts and law enforcement representatives of the 188 INTERPOL member countries.

A recurrent theme in many speeches during the two-and-a-half days was public-private cooperation. This was reinforced by the participation of local speakers, including Roy Ko of HKCERT, LegCo Member Samsom Tam, Frank Yam of ISACA and Yui Kee Chief Consultant Allan Dyer, representing the Hong Kong Computer Society.

Mr. Dyer spoke on Critical Infrastructure Protection during a Day 1 Panel Session in the Technical Track, a theme picked up on by Samson Tam in his Keynote speech on Day 2. Samsom Tam emphasised the need for increased funding, and the role of HKCERT.

Demonstrating their versatility, all but one of the performers at the Gala Dinner were Hong Kong Police Officers

The conference ended by agreeing five recommendations to strengthen information security capacity.

More Information

Critical Questions on Critical Infrastructure
The 1st INTERPOL Information Security Conference
Photo Highlights

Malware: The Anti-Personnel Mine of Cyberwar

<web-link for this article>

Allan Dyer

An article in today's South China Morning Post describes Stuxnet as 'world's "first cyber super-weapon"', but it seems to me that malware is much more like anti-personnel mines: cheap, dirty, and goes on injuring innocents long after the conflict they were deployed for has ended. True, Stuxnet is a shining example of sophistication, but it has still spread to thousands of systems across the world, including Iran, Indonesia, Germany, India, and now, as the Post reports, China. How many of those were the intended targets? The leading conspiracy theory is that Stuxnet was deployed, by a major Government, to damage Iran's first nuclear plant at Bushehr. Assuming this is true, what was the justification for the "collateral damage" to Chinese, Indonesian, German and India industrial plants?

Another parallel with malware is the list of countries that have not joined the Ottawa Treaty, which bans the use, production, stockpiling, and transfer of anti-personnel mines: United States, Russia and China. These states, that are arrogant enough to insist that they should be allowed to deploy indiscriminate weapons of dubious military value regardless of the humanitarian issues, are also accused of being most aggressive in the development of cyberwar: China for Operation Aurora and Titan Rain, USA for Stuxnet and Russia for network attacks in Estonia and Georgia. But, just like an unmarked mine, there is only circumstantial evidence of their involvement.

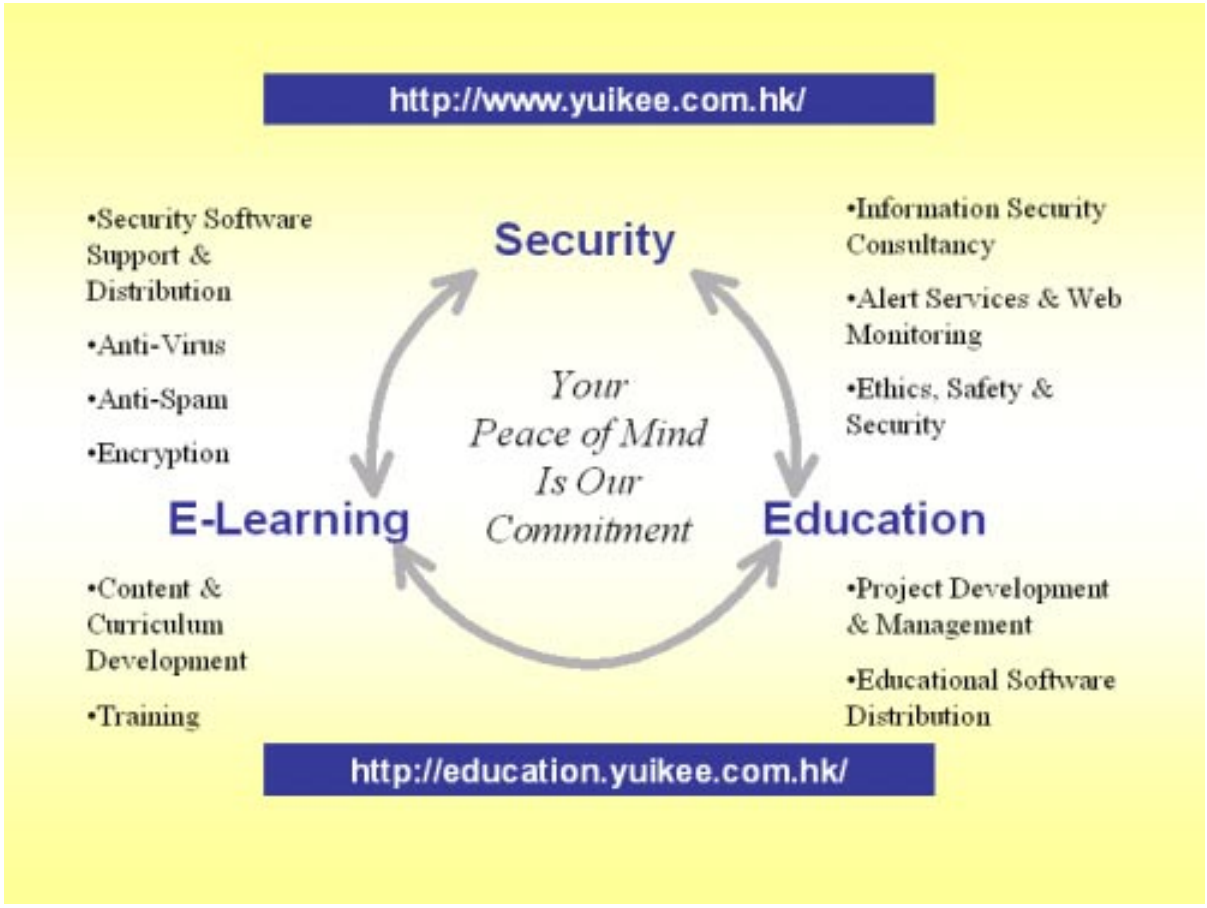
Enough of the metaphors, cyberwar's cost is merely economic. No malware has ever blown off a child's hand while they played.

More Information

Cyber worm hits mainland industry
Critical Questions on Critical Infrastructure

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/