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

Yui Kee Computing Ltd.

Newsletter

November 2009

Contents

Hong Kong Amends Strategic Commodities Import and Export Regulations

<web-link for this article>

Hong Kong's Trade and Industry Department has announced an amendment to Schedule 1 of the Import & Export (Strategic Commodities) Regulations in Strategic Trade Controls Circular No. 16/2009. The amendment includes four changes to the regulations on Information Security products:

- 5A002(a)(7) - Add the control on certain non-cryptographic information and communications technology security systems and devices.
- 5A002, Note(h) - Relax the control on certain equipment designed for servicing of portable or mobile radiotelephones and similar client wireless devices with cryptographic function.
- 5A002, Note(i) - Relax the control on certain wireless personal area network equipment with published or commercial cryptographic standard.
- 5B002(a) & (b) - Relax the control on certain information security test equipment.

The changes will take effect on a day to be appointed by the Director-General of Trade and Industry by a notice published in the Gazette.

More Information

Strategic Trade Controls Circular No. 16/2009
Highlights of the Import and Export (Strategic Commodities) Regulations (Amendment of Schedule 1) Order 2009

COFEE: Who Spilt the Beans?

<web-link for this article>

Microsoft's free law-enforcement-only live forensics tool, COFEE, has been posted to a file-sharing site, in violation of the license conditions. Microsoft has downplayed the leak, Richard Boscovich, senior attorney for Microsoft's Internet Safety Enforcement Team said, "we do not anticipate the possible availability of COFEE for cybercriminals to download and find ways to 'build around' to be a significant concern", adding that it is a simple, customisable collection of forensic tools, "already commonly used around the world".

Graham Cluley, Senior Technology Consultant at Sophos, asked in his blog, "what's to say that the bad guys couldn't analyse COFEE, and write their own code which neutralises it (or wipes sensitive data from their computer) if they determine it is being run on their own computer?".

Hong Kong Police were an early adopter of COFEE.

More Information

Microsoft's COFEE forensic tool leaks onto the web
Computer Online Forensic Evidence Extractor (COFEE)
Hong Kong Police use Microsoft's COFEE Live Forensic Tool
Microsoft Forensics Tool For Law Enforcement Leaked Online

Humour - Cloud Computing Security

<web-link for this article>

Dilbert advocates encryption for cloud computing, and less pointy-ears.

More Information

Dilbert comic strip for 11/19/2009

The Evolution of Network Security at AVAR 2009 in Kyoto

<web-link for this article>

Allan Dyer

The twelfth Anti Virus Asia Researchers Annual Conference took place in Kyoto, Japan on the 5th and 6th November. The conference had about 300 attendees, and many of the best-known names in the Anti-Virus industry. The importance of the event was underlined by a keynote speech from Seishu Makinoa (牧野聖修) member of the House of Representatives of the National Diet of Japan (国会).

AVAR Chairman Seiji Murakami

Jimmy Kuo of Microsoft presented the Key Findings from Microsoft's recently published Security Intelligence Report covering the first half of 2009. The data is, arguably, the

Seishu Makinoa (牧野聖修) member of the House of Representatives of the National Diet of Japan (国会)

largest dataset of Windows malware information, coming from Microsofts' various security tools, protected web mailboxes and scanned webpages. Miscellaneous trojans (including rogue security software remained the most prevalent category, but worms and password stealers also rose in prevalence. Asia was a hot area for malware distribution sites.

A major theme was the enormous numbers of new malware (about 2 million unique sample files a month, according to one developer, and 1883 new threats an hour, according to another), and how to deal with that. Andrew Lee discussed "Threat for a Day", and how the fast appearance *and* disappearance of threats required a paradigm shift in our approach. Several papers looked at automated processing of malware: "MCNS: Intelligent Malware Categorization and Naming System" by Yangang Ye, Winming Mei and Renchang Pang; "Feature Extraction, Classification and Learning for Malware Codes" by Kazuki Iwamoto.

Shigeru Ishii AVAR2009 Conference Chairman

Jimmy Kuo presenting Microsoft's report

Several technical papers examined the tricks used by malware authors: Jie Zhang looked at scramblers, Masaki Suenaga considered Win32 API obfuscation and Satyendra Teppalavalasa discussed PDF attacks.

But not all tricks are technical, Stefan Tanase compared social networking to viruses, and explained the types of attack becoming prevalent on Facebook, Twitter and other social networking sites and Shin-ichiro Kagaya explained the development of "One-click Billing Fraud", a trick peculiar to Japan, that uses embarrassment to discourage reporting of fraudulent websites. Katsuyuki Okamoto took the Web 2.0 thread to the detection side and discussed correlation in the cloud.

It is not only developments by the bad guys that can cause problems for AV software. Abhijit Kulkarni and Prakash Jagdale looked at Windows Vista's Transactional NTFS (TxF), and how that can prevent a real-time Anti-Virus scanner from detecting a virus being written to a file. For virtual environments, Shuveb Hussain showed how to achieve Hypervisor Security.

Prompted by Dr. Cohen's soundbite at the EICAR conference that viruses and malware will become the preserve of nation states and will be considered munitions, and related news, such as "cyberwar" in Estonia and Georgia, and calls for an "Internetpol", I moderated an interesting panel on Government Involvement in Anti-Virus with Vincent Weafer, Dmitry Gryaznov, David M. Perry, Randy Abrams and J.Kesavardhanan. The quote of the panel, neatly summarising the consensus that while improved cooperation between Government, the AV industry and users is important, it is clearly infeasible to regulate malware like tanks, was by David

Charles Ahn

Andrew Lee explaining Threat for a Day

Perry, "I don't know what [Dr. Cohen] was smoking that day".

Abhijit P. Kulkarni and Prakash D. Jagdale on the Darker Side of TxF

Another question is how to test AV as it changes to meet tomorrow's challenges, Wei Yan presented a methodology to credit AV products that use web reputation services to protect against web threats.

Ian McMillan reported on the continued development of Microsoft's Automated Scanning Service, which has the twin goals of zero malware, and minimising false positives in Microsoft's product releases.

On day two, Suguru Yamaguchi gave a Keynote on Information Security in the time of "Complexity". Hidehiro Yajima then moderated a panel comprised of Masanori Saito, Masayasu Nakano and Yasuhide Yamada discussing Information Security policy in Japan.

A new feature of this year's conference were the Gallery Sessions, which ran parallel to the main stream, in a more relaxed, smaller setting, but without simultaneous translation. Several of the Gallery Sessions were workshops, or tutorials.

The Gala Dinner was an excellent Japanese banquet, with Maiko (舞子) dancing and a very energetic drum and flute performance.

The AVAR2010 conference will take place in Bali Indonesia.

Motoi Endo explain effective anti-virus in the Gallery

More Information

Security Intelligence Report v7 is Now Available
SIR Volume 7 (January through July 2009) and Key Findings Summary (available in 10 languages)

Views on the Review of the Personal Data (Privacy) Ordinance

<web-link for this article>

Personal Submission by Allan G. Dyer

Introduction

This submission addresses the review of the Personal Data (Privacy) Ordinance (PDPO), and the consultation document published by the Hong Kong Government on 28th August 2009. The areas include the limited scope of the review, comments on most of the Proposals in the Consultation Document and further discussion on biometrics.

Copyright, Privacy, Obscenity and Free Speech

In January 2009, I made a submission[1,2] to the Review of the Control of Obscene and Indecent Articles Ordinance, saying, in part:

> *"It is clear that different people hold a wide range of views on what personal information (including images) they want to record and, optionally, make public, and the view might change according to the circumstances. Similarly, there are many views on public decency and obscenity, and the location can change the standards. In the current situation, laws intended for other purposes are sometimes used to try to address these emerging issues. In the early stages of the Edison Chen scandal, it was suggested that websites publishing the photos should be prosecuted under the COIAO, despite the fact*

> *that the images were of a similar nature to many erotic images on the internet. Should an obscenity law be used to protect privacy? Now, copyright law is being used against the perpetrators, but copyright was originally intended as a trade: creators get exclusive rights for a limited period and Society benefits from the creations when copyright expires and they pass into the public domain. Why should that be used for images that were intended solely for private enjoyment?"*

The Edison scandal is over, but the issue remains, and reappears in other, less high-profile cases: cases that are essentially about Privacy are being forced into fitting other definitions (Copyright or Obscenity, in this case) because the PDPO is too weak on enforcement.

Copyright, Obscenity, Privacy and Free Speech are all related to the control of information and are interlinked in complex ways. The complexity cannot be addressed by a limited review of the PDPO, I quote again from my submission[*ibid.*] to the Review of the Control of Obscene and Indecent Articles Ordinance:

> *"A new Review should be launched, with a scope that covers all the closely related areas: Telecommunications and the role of ISPs, Privacy, Copyright, and Obscene and Indecent articles."*

Proposal No. 1: Sensitive Personal Data

Imposing more stringent regulation on personal data because it is "sensitive" implies that disclosure of some information is inherently more damaging than the disclosure of other information. This is untrue: a person attending a trade union meeting, or a Mass at a Catholic Cathedral, or drinking in a gay bar is displaying biometric information (their face) in a public place, and providing a strong indication of their membership of a trade union, or religious beliefs, or sexual life, yet the disclosure is (usually) harmless. It is how the information is (mis-)used that makes the difference. Conversely, home address is not listed in the examples of "sensitive personal data", but disclosure of it to a loan shark could be extremely damaging for the individual concerned.

It would also be wise to consider the implications of classifying biometric data as "sensitive" and probable future improvements in technology. Classifying racial origin, and health condition as "sensitive" necessarily makes genetic information "sensitive", because our genetic information records our racial origin, and our inherited diseases. In future, it might also be possible to predict a person's facial features or fingerprints from their genetic information. However, we all constantly shed genetic samples, most commonly in the form of dead skin and hair. House dust is mostly comprised of dead skin cells. The bag of a vacuum cleaner contains a record of the people who have been where it has cleaned and it might soon become feasible to extract that information. Will we require cleaners to follow strict data disposal protocols, or will we focus on how information is processed and used?

Biometric data, and how it can be disclosed, is considered further in section 15 .

The protection of personal data should not depend on whether it is included on a list of "sensitive" data because the potential damage depends too much upon circumstances, and because the more stringent controls will, inevitably make normal activities, such as cleaning, impossible.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

There appear to be, broadly, three categories of Data Processor that are affected:

1. Commercial contractors and sub-contractors;
2. Service providers that do not use the data themselves, including ISPs and search providers;

3. Social networking sites and other internet-related businesses that process the same data for multiple users.

Of course, these are not rigidly-defined categories, and one organisation might fall into more than one category, depending on the circumstances.

For the first category, the Data Users and the Data Processors have (or should have) the technical expertise to understand the issues, and the power to negotiate the contract to comply with the law. In that case, the Data User should be required to use contractual or other measures to secure compliance; and the Data Processors should be directly regulated in their obligations.

For the second and third categories, the Data Users (individuals and SMEs) do not have the power or technical expertise to negotiate with the Data Processors – at best, there will be a "take-it-or-leave-it" End User Agreement. My submission on the Review of the COIAC[ibid.], section 3.1 included a discussion of an overly-restrictive ISP End User Agreement, if the same restrictions on Data Processors, intended for Contractors were applied to ISPs, then, no doubt, ISPs would find it necessary to protect their interests with even more restrictive End User Agreements.

The law should regulate limitations on the agreement so that Data Users are not faced with either blindly accepting impossible conditions, or being excluded from the Information Society.

So, for the second category, ISPs and search providers, a balance can be achieved by exempting them from most PDPO provisions, but not from ensuring the same level of security that the data had (if a website publishes private information to the world, it is not reasonable to prosecute a search engine for indexing it), while restricting their End User Agreements.

For the third category, social networking sites, it is a lot more complicated because the Data Users include not just multiple individuals and the site provider, but also third-party application (often game) developers, that may request and require users to allow access to their profile before they can play the game. The biggest issue here is that there is a lack of transparency about who is getting access to which data. The Data Protection Principles, particularly DPP1, DPP3 and DPP5, address this issue already, but social networking sites are often based outside of Hong Kong, and there have been no legal cases covering this area in Hong Kong so there is no guidance on best practice for those involved. This could be improved by:

1. Giving the Privacy Commissioner the power and resources to start an investigation without having received a specific complaint.
2. The Privacy Commissioner preparing Guidelines for Social Networking sites, and, in the future, whatever new types of internet-based businesses that appear.

Proposal No. 3: Personal Data Security Breach Notification

A voluntary privacy breach notification system is worthless – the worst offenders will not volunteer so the additional costs caused will be a burden only on responsible organisations. Responsible organisations will therefore be less competitive in the Free Market, and irresponsible organisations will succeed, the exact opposite of what is desired. Therefore, there should be a mandatory breach notification system.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

There appears to be insufficient reason to concentrate the additional power of prosecution in the Privacy Commissioner.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

The power to provide legal assistance would greatly enhance the effectiveness of the PDPO.

Proposal No. 6: Award Compensation to aggrieved Data Subjects

While deciding on and awarding compensation may be best left to the courts to decide, it should be noted that the process of noticing, researching, reporting and following up on a possible breach of the PDPO can be time-consuming for a Data Subject. For example, in Case No. 200214122[3] a Data Subject noticed a potential security flaw on a website, tested that it actually existed, and reported it to the Privacy Commissioner. After investigation, the Commissioner required the website owner to improve the security and asked the Data Subject whether the changes made were sufficient. The Data Subject identified new flaws and reported them but also expressed the view that it is not his intention to do unpaid security consultancy for the website owner.

Notwithstanding any claim for compensation, it would be appropriate, when an Enforcement Notice is issued, for the Privacy Commissioner to require the culprit to recompense the reporter a reasonable fee for the service of reporting the breach of the PDPO.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

The biggest weakness in the PDPO currently is the Enforcement Notice system whereby personal data can be negligently or maliciously disclosed, with potential of actual damage to the Data Subject(s), and the Privacy Commissioner is essentially limited to saying, "Naughty, naughty; don't do it again"!

Disclosure of information is non-reversible, once published, it cannot be "un-disclosed" and the damage caused cannot be undone. The Edison Chen case illustrates this dramatically: the culprit who copied the files without permission has been sentenced[4] yet the pictures are still locatable on the internet, and the subjects' careers are still in tatters. In addition, maybe Edison was negligent in storing such sensitive information with insufficient protection.

The Enforcement Notice system may work adequately in allowing the Privacy Commissioner to review the handling of personal data in responsible organisations, and recommend improvements in-line with the DPPs, for example, when the Privacy Commissioner ordered a school to stop fingerprinting children[5]. However, it ceases to be effective as soon as negligence or malicious intent are involved. In particular, when there has been an actual data leak, with potential or actual damage to the Data Subjects, there should be penalties to act as an effective deterrent.

Over the past couple of years, there have been a string of data leak incidents: from an IPCC contractor[6], from Hospitals, the Immigration Department, and HSBC, but no penalties for the negligent organisations and staff. This sends a clear message: don't bother about protecting personal data until you receive an enforcement notice.

Proposal No. 8: Unauthorised Obtaining, Disclosure and Sale of Personal Data

Breach of DPP3 is one of those areas where, as discussed above, in Section 9 , the Enforcement Notice system is inadequate, and it should therefore be an offence. The defence provisions used in the UK appear reasonable.

However, it should be noted that "identity theft" is, in general, an offence enabled by the negligence of Data Users that inappropriately use personal data for the purpose of authentication. It would not matter that a criminal could discover your mother's maiden name or the name of your first pet if you bank did not use that information for their "security questions". Disclosure of other biometric data is discussed in section 15.

The Privacy Commissioner should make it clear that inappropriate use of personal information for authentication contravenes DPP1 ("Only personal data that are necessary for or directly related to the purpose should be collected") and DPP4 (security of personal data), and should issue Enforcement Notices to organisations, particularly banks and financial institutions (where the potential loss is greatest) that are negligent about this.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

From a casual reading of the Privacy Commissioner's website, and other documents, it is not clear that this loophole exists. However, if it does, it is a serious flaw that should be fixed as soon as possible. The fact that no cases have occurred is irrelevant: a Data User that did this would be flouting the intent of the law with clear premeditation and there must be a strong motive for the action. The penalty level should be the same as simple non-compliance.

Proposal No. 10

No comment.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

A repeated offence should attract a heavier penalty.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Before raising the maximum penalty, it should be considered whether making the penalty proportional to the number of Data Subjects that were victims would be effective. Thus, if a direct marketer misused an address list of 10,000 people, the magistrate could impose a fine of up to $10,000 for each person affected, which is 10,000 x 10,000 = $100,000,000 in total. If the base penalty is commensurate with the damage to the individual victim, then the total penalty will be commensurate with the damage to Society. Organisations that hold, and (mis-)use, data on individuals should realise that their responsibility grows with the number of individuals.

Biometric Data and Authentication

We all constantly disclose our biometric data in numerous ways – genetic information in dust has already been mentioned in section 3, we disclose our face simply by walking down the street, and leave our fingerprints on each door handle and handrail we touch. More permanently, in the Hong Kong Polytechnic University there is a wall featuring the handprints of distinguished donors where the fingerprints are clearly discernable, and quite possibly recoverable. Should the wall be demolished, and we all be required, by law, to wear masks and gloves in public?

The problem is not in the disclosure of the information, but in the processing and use of it. Biometrics is frequently seen as the panacea for authentication problems when, in reality, it provides a (at best) unique identifier, not an authenticator. It is only under carefully-controlled conditions, such as in the Immigration halls at our borders, that the connection between identity and authorisation can be reliably made.

Conclusion

The current PDPO restricts the Privacy Commissioner to being ineffective. No matter the severity of the case, he or she can only issue an enforcement notice in the first instance. The current situation means that there is little incentive for organisations to improve their handling of personal data, before an incident occurs. We have therefore seen a continued series of headline-grabbing incidents.

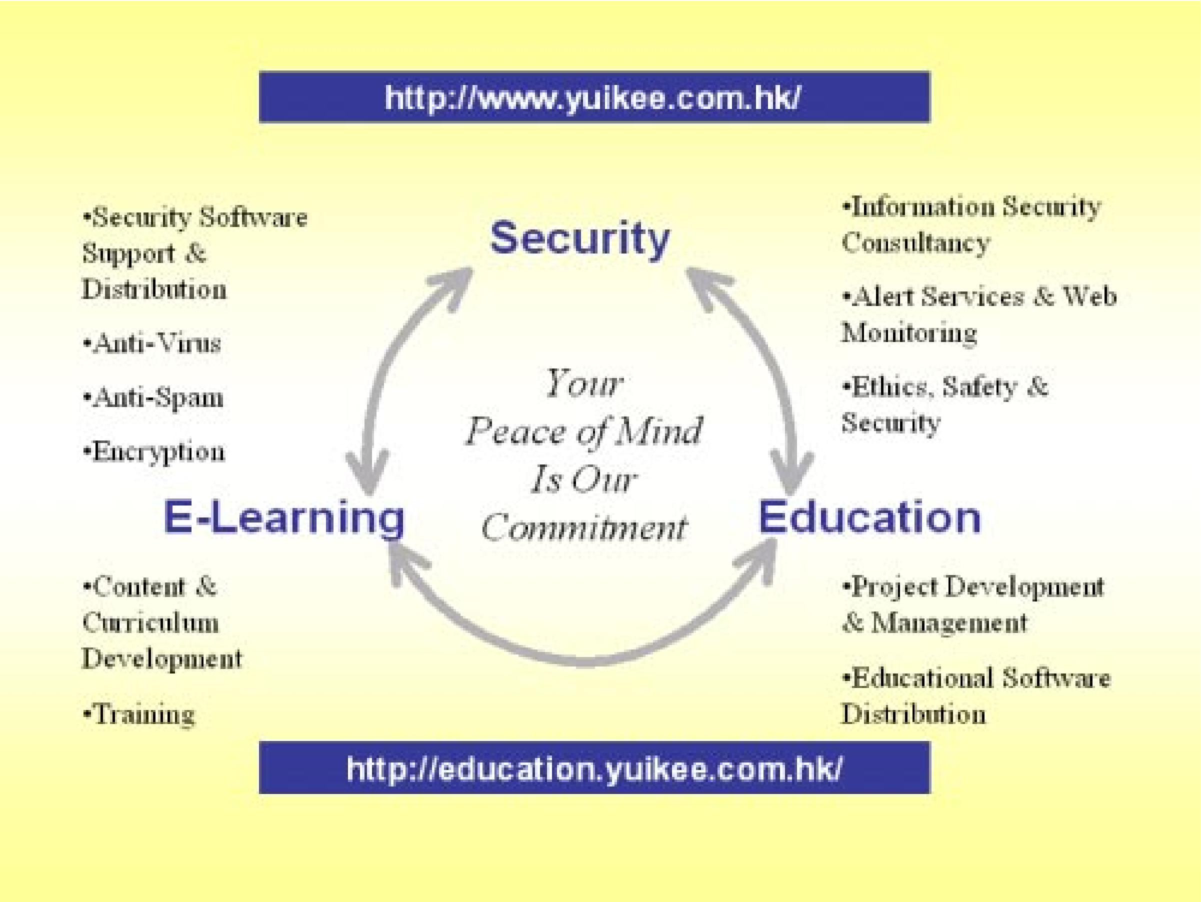
The implications of Social Networking and similar internet-based applications with numerous data users are a concern and should be considered in detail.

More Information

Volume 39 of the written submissions received during first round consultation of the Review of the Control of Obscene and Indecent Articles Ordinance
Views on the Control of Obscene and Indecent Articles Ordinance
Privacy Commissioner tells Mobile Operator to Improve Website Security
8½ Months Jail for Sex Photo Techie
HK Privacy Commissioner on Fingerprinting in Schools
IPCC Data Leak
Privacy Commissioner Recommends Improvements at the Hospital Authority
Data Leak Disease

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 Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
Security
•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/