Yui Kee Computing Ltd.

Newsletter

October 2019

Contents

Information Security Summit in Hong Kong

<web-link for this article>

The 16th Information Security Summit will be held at the Hong Kong Convention and Exhibition Centre on 23 and 24 October. With the theme, "Over the Horizon Cyber Security", the two day conference is a Regional Event with the aim to give participants from the Asia Pacific region an update on the latest developments, trends and status in information security. Conference registration is free, there are also a series of nine workshops, running from October to January, on demonstrating management and technical theory, applications and practical experiences on all aspects of information security relating to securing and protecting data in borderless cloud and mobile environment, big data analytics and the Internet of Things.

As cyber attackers are growing more capable and smarter, enterprises are looking at investing in analytics and threat intelligence in order to make better decisions on investment in cyber defence to pre-empt the attacks. Advanced security technologies are increasingly integrated with threat intelligence. Overseas and Local Experts from the industry have been invited to share their experience and knowledge.

Speakers and Organisers at the opening ceremony of the Information Security Summit

The event is organised by the Hong Kong Productivity Council and supported by HKCERT, HK Computer Society, Cloud Security Alliance, High Technology Crime Investigation Association, HK Information Technology Federation, Professional Information Security Association, Internet Society (HK Chapter), Information Security and Forensics

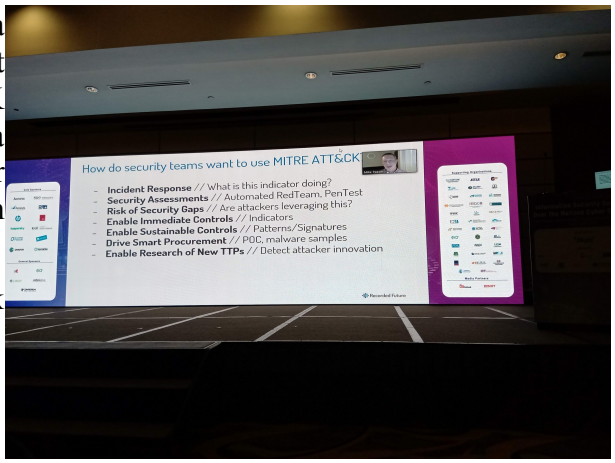
Society, International Information Systems Security Certification Consortium, and Information Systems Audit and Control Association.

Updated: 25th October 2019

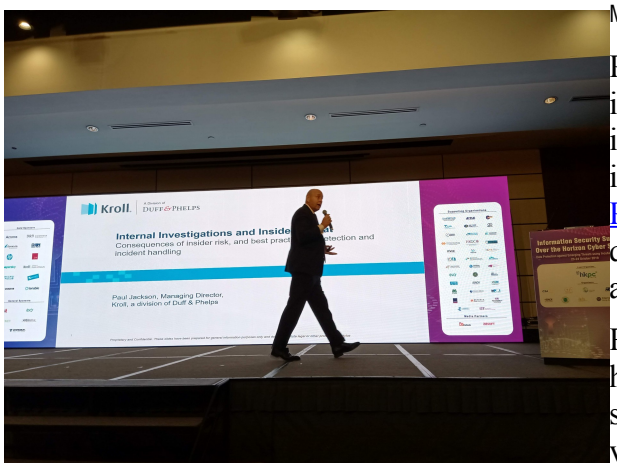
In the first keynote speach, Pishu Mahtani from (ISC)^2 highlighted the problems with security on the Internet of Things (IoT). He advocated Security by Design (locking down production devices against physical attacks), by Default (avoiding weak default credentials) and by Deployment.

Mike Passaro from Recorded Future gave a remote presentation on applying threat intelligence to the MITRE ATT&CK framework. The ATT&CK framework is a knowledge database describing cyber adversaries and providing a common taxonomy for offence and defence.

Leo Chan of Tenable demonstrated how risk exposure and vulnerability are determined.



Mike Passaro explaining the MITRE ATT&CK framework



Paul Jackson marches on Insider Risk

Paul Jackson of Kroll Associates gave his insights on the increasing prevalence of the insider threat, and how to approach investigations. He introduced Kroll Artifact Parser and Extractor (KAPE), a free tool for quickly collecting key incident information across a variety of systems.

Richard Hollis of Risk Crew limited highlighted how badly we are addressing cyber security; the OWASP list of top ten exploited vulnerabilities is almost unchanged since 2013. Attackers have moved from the familiar scenario of utilising an attack vector to deliver a payload to achieve a target to a multi-stage, cyclical process designed to make APTs a persistent, moving target. He argued that we are facing an iceberg of data loss: what we see, the loss that is reported, is only a small fraction of the total. He advocated greater accountability for data loss.

Sean Duca of Palo Alto Networks talked about how the Internet of Things threatens our security and zero trust design concepts to address that.

Jason Yuan of Sangfor presented their approach to combatting ransomware.

Day one ended with a lively panel session moderated by Paul Jackson and featuring Sean Duca, Richard Hollis, and Pishu Mahtani

Day two started with a keynote from Roy Ng of Centre for Research in Information Assurance (CRIA) on how 5G will be a paradigm shift in cyber security. He advocated rethinking countermeasures with an information assurance model and machine for holistic protection.

David Gee of HSBC explained their approach to cyber risk quantification using probability distributions as coefficients in their model so that the findings are presented with the

associated uncertainties. They use the findings to direct their cyber security investment to the most effective risk reducing controls.

Jeffrey Carpenter of SecureWorks shared his experience from recent incidents and the challenges his clients faced. He emphasised that "exciting" attack vectors are not the ones you should worry about the most. The currently most prevalent cybercriminal threats are business email fraud, ransomware, digital currency mining, and banking trojans. Ransomware attacks are evolving to increase their impact, and therefore the potential gain for the attacker, by spreading laterally within the victim's network before revealing themselves. He highlighted lack of Cyber Hygiene as an industry crisis. This includes deficiencies in password policies, patching, authentication, allocation of user privileges and administration rights, and hardening.

The panel discussion before lunch on emerging security threats featured Mika Devonshire, Andrea Lau and Carol Lee and was moderated by Anna Gamvros.

Anna Gamvros, Mika Devonshire, Andrea Lau and Carol Lee discuss emerging threats.

Andrea Lau of Security Research Labs reported on the challenges of security during the rollout of the Jio Network in India: their pilot test was with 1 million staff and their families, the full rollout covered hundreds of millions. One issue was that even the new equipment was arriving with old vulnerabilities, such as core network devices unpatched since 2007. User inexperience was also a problem, with the majority of users falling for phishing and vishing attacks in tests. She concluded that "security by design" is a dream when even a 100% greenfield startup is tied to insecure legacy in equipment and employees.

Mika Devonshire of Blackpanda talked about Cyber Liability Insurance and how it fits in with cyber security with particular reference to ransomware trends.

Michael Mudd moderated the final panel, on the future of information security, with Roy Ng, Jason Yuan and Jeffrey Carpenter. The organising committee char, Dale Johnstone, closed the summit with a few remarks.

More Information

- Kroll Artifact Parser and Extractor (KAPE)
- Information Security Summit - Over the Horizon Cyber Security
- Workshops

Personal Privacy and the Free Flow of Information

<web-link for this article>

I was honoured to be invited to speak as a foreign expert at the International Anti-Virus Conference 2019 (IAVC 2019) at the Tianjin Meijiang Convention Center, Tianjin, China in September. The theme of IAVC 2019 was "Cope with New Challenges of Anti-virus and Promote Personal Privacy Protection" and I started to prepare my speech around hot topics in information security and personal data privacy, with particular reference to my home city,

Hong Kong. However, I was advised that certain parts of my speech were a sensitive topic in China and asked to remove them. I presented my speech without the sensitive topic, but I believe that the only way we can successfully face difficult situations is with the best available information, discussed rationally. Hong Kong is a part of China that, under the Basic Law, enjoys the freedom of speech, of the press and of publication, therefore I present here the topic that was deemed too sensitive for Tianjin. This is based on an early draft of my speech for IAVC 2019, edited for the medium and with the addition of relevant later events:

Privacy

Personal privacy has had legal protection in Hong Kong since 1996, when the Personal Data (Privacy) Ordinance came and the Office of the Privacy Commissioner for Personal Data is an an independent statutory body set up to oversee enforcement. Each year in May they hold Privacy Awareness Week, with various educational events for all sectors of society. However, there have been serious data breaches.

Cathay Pacific

In October 2018, Cathay Pacific reported a data breach that exposed personal data of 9.4 million customers, included me. Cathay Pacific offered the victims a free identity monitoring service, provided by Experian, a company that had their own data breach between 2013 and 2015. In November 2018, Cathay Pacific faced a panel of Hong Kong's Legislative Council (LegCo) to answer questions about the breach. At that meeting, they reported that the attacker used previously unknown malware and utilities in the attack, which Cathay's up-to-date anti-virus system did not detect. Cathay has had in place detection and monitoring systems to detect APTs, and in March 2018 they also implemented an advanced endpoint detection and response system.

I think this data breach shows us that personal data is an attractive target for criminals. The data potentially has multiple uses, not all of them criminal. The most sensitive information: passport or credit card numbers, can used in fraud but other information can be used by marketeers to target ads. Even a list of valid email addresses can be sold multiple times, and where is the proof that they came from a data breach? A company will have strong protection for their financial systems and research and development, and access will be limited to a small team. Personal data will have "ordinary" protection, and be accessible to multiple teams: customer service, marketing. If you steal top secret plans, you will need to find a dishonest competitor to sell them to, but personal data can be sold in many more ways.

Patient Privacy

Medical data is very sensitive. In June this year, it was revealed that patient data in Hong Kong's public hospitals was insecure. The problem is with a program, called AEIS, used in Accident and Emergency departments. A user could bypass the normal login through the use of a short cut on the computer’s start menu. A black window popped up to launch AEIS, also known as the Accident and Emergency Department Clinical Information System. From there, patients' details could be examined and printed.

Privacy Commissioner for Personal Data Stephen Wong Kai-yi said on Monday his office had launched a compliance check to determine if a login was required to gain access to patients’ personal information at emergency wards in hospitals under the authority.

Dr Chung Kin-lai, the Hospital Authority’s director in quality and safety, admitted that logging in to the system was not required, but stressed it had never authorised anyone to print patient data for police. He said patient information would be given to police in only two circumstances: when a patient list would help the police account for injured or missing people; and when a hospital needed police help to contact a patient’s family.

The Hospital Authority has announced a task force would be set up to identify ways to protect patients' medical information.

Doxing

In 2017-2018 reporting year, the Privacy Commissioner received 1619 complaints of which 16 were referred to the Police for criminal investigation, but between 14 June 2019 and 26 July 2019, 430 cases of Online Disclosure of Personal Data were referred for criminal investigation.

The massive rise is related to the current social unrest in Hong Kong. In a few cases, student leaders and their families have been threatened anonymously with violence. Most cases have involved Police officers, Government officers and other public figures, and their families.

"Doxing (from dox, abbreviation of documents) is the Internet-based practice of researching and broadcasting private or identifying information (especially personally identifying information) about an individual or organization."

During the protests, Police officers in the special tactical unit have been observed without number badges. A vice-chair of the Independent Police Complaints Council (IPCC), has said that those officers may be hiding their identification documents over privacy concerns. However, this raises an important difference between personal privacy and personal responsibility. The badge numbers are there so that officers can be held responsible for their actions while on duty. The only link between the number and other aspects of their identity, such as their name, address or family members, is held by the Police. Revealing the badge number does not put their sensitive personal data at risk. This can be compared to the Hong Kong ID card number, which is widely used for many purposes. It is used by schools as the student number, at the Companies Registry to identify Directors, for bank accounts, and it is recorded at the security desk of some buildings. Some ISPs and phone companies use it as a default password. Therefore, disclosure of a Hong Kong ID card number allows many other pieces of personal data to be linked from different sources.

On 23 October, the Hong Kong Junior Police Officers' Association won an application for an injunction barring the public from checking personal details on the voters' register. On 25 October, the Department of Justice and the Police Commissioner were granted an interim injunction to ban the release of any personal information of police officers. On 29 October, Police have announced that frontline officers will wear white identification tags with "operational callsigns" which are unique to each officer. These changes introduce some clarity about the difference between a unique identifier and protected personal information; and limit the exposure of sensitive personal information of officers and their families. However, it leaves the question of why Police officers are granted additional protection when other members of the public who may be more vulnerable are not. Also, there should be a full discussion of the implications of restricting access to the voters' register. An accessible voters' register supports free and fair elections by allowing people qualified to vote to verify that they are correctly registered before an election takes place, and it allows potentially fraudulent registrations to be identified, for example, if an enquirer notices that there are additional registrations for people not resident at their address, or registrations for voters who are deceased. It should be noted that the Online Voter Information Enquiry System" (OVIES) remains functional. The OVIES regulations claim that it only allows an elector to check his or her own registered particulars. In reality, the enquirer must know the HK ID number and full name of a person, and be able to correctly identify two items from their address from a list. This then reveals the constituencies that the person is registered to vote in.

There is a tendancy for organisations to collect ever greater amounts of personal data, but these cases in Hong Kong show some of the dangers. Although the data you are collecting has a legitimate and useful purpose, it is also necessary to consider how it could be linked to

other collections and how the data could be mis-used in combination. Even if your data store has limitations and security in place, could poor security on another data store be leveraged against your security? We need to be thinking more about how to break up personal data and limit how it can be combined.

Facial Recognition

In the UK, many organisations, including the Police and commercial companies such as shopping malls have been deploying facial recognition for several years. However, there are increasing calls for debate and restrictions on how it is used.

This month, the Ada Lovelace Institute released a report on public attitudes to facial recognition technology in the UK.

One of the key findings was that the ability to consent, or opt-out of, facial recognition technology was seen as an important safeguard.

Another was that people see a trade-off between public benefit and the normalisation of surveillance. While they might accept its use in criminal investigations, use in schools or public transport was much less acceptable.

Facial Recognition Concerns

The report also highlighted some concerns about the limitations of facial recognition technology.

One was that live trials of the technology by Police resulted in 90% incorrect matches. Supporters of the technology point out that, while this is a high error rate, the procedure would be to stop and question the person, and let them go as soon as it was clear they were not the wanted person. However, I think that the errors are unlikely to be evenly distributed. A few people, who happen to be similar to wanted people, will find that they are frequently stopped and questioned.

A second concern was that the technology tended to be less accurate for minorities. This is probably simply a consequence of how the systems are developed: the set of training data favours the majority. Although the explanation is innocent, the result could be serious discrimination against minorities where they are subject to more frequent misidentification.

Personal Data and Recognition

Another complexity is that identifying a person in a photo or video, whether by eye or by technology, might change the images into Personal Data, protected by law. After an incident in an MTR station, the MTR Corporation refused to release video from surveillance cameras on the grounds of personal data privacy. However, David Webb pointed out that in a landmark case in 2000, the Court of Appeal noted that photographs taken and published of people whom the publisher does not identify (or even know the identity of) are not "personal data" within the meaning of the PDPO.

Allan Dyer

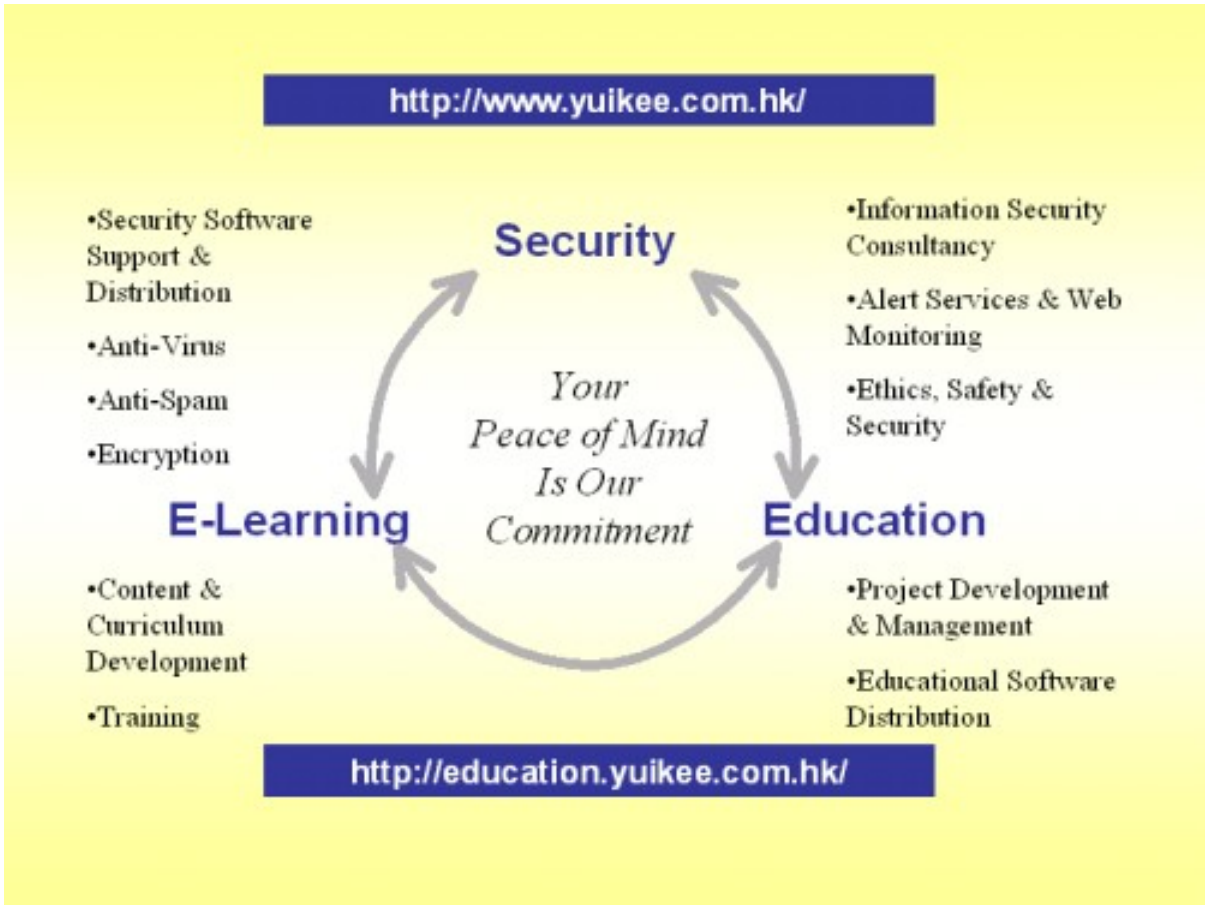
More Information

- Privacy Awareness Week 2019
- Hong Kong government weighs in on Cathay Pacific data breach, urging airline to cooperate with privacy watchdog in investigation | South China Morning Post
- Hong Kong police visit Cathay Pacific HQ to investigate major data breach that hit 9.4 million customers | South China Morning Post
- Cathay Pacific to Face LegCo Panel on Data Leak

- Hong Kong youngsters not minding web privacy, survey finds | South China Morning Post
- Hong Kong Hospital Authority denies leaking data to police after extradition bill protesters arrested in public hospitals | South China Morning Post
- Hong Kong Hospital Authority values patient data privacy, and police are not given access rights to information systems | South China Morning Post
- Leaked video exposes how patient data in Hong Kong public hospitals can be accessed by any user without needing a password | South China Morning Post
- Hospital Authority vows to revive public trust as stories emerge of protesters arrested after personal details leaked by city-run facilities | South China Morning Post
- Enforcing Data Protection: PDPO Report 2017-2018
- Criminal Investigation Procedures Commenced on 430 Cases of Online Disclosure of Personal Data in Accordance with the Law
- Privacy Commissioner Has Started Reviewing Related Websites and Urges Netizens to Respect Others' Privacy
- Privacy Commissioner's Response to Suspected Disclosure of Personal Data of Government Officials, Legislators and Police Officers at Online Discussion Forums and Instant Messaging Platforms
- Uphold Unique and Irreplaceable Attributes of "One Country, Two Systems" Advocate Privacy Accountability and Data Ethics Privacy Commissioner Speaks at IAPP Asia Privacy Forum in Singapore
- Privacy Commissioner's Response to the Display of Police Officers' Personal Data in Public Places
- Privacy Commissioner responds to media reports on open letter issued by purported PCPD staff
- 'We know where you live': Hong Kong student leaders and their families face anonymous threats
- Tactical squad may be hiding IDs in order to protect privacy, says Hong Kong police watchdog vice-chair
- Police forces halt trials of facial recognition systems
- Beyond face value: public attitudes to facial recognition technology
- Hong Kong's MTR releases CCTV screenshots to calm rumours of police raid fatalities, but full footage under wraps
- MTR videos are not Personal Data under PDPO
- Hong Kong police assoc. wins injunction application barring public from checking voter registers
- Hong Kong court orders temporary ban on the release of police officers' personal information
- Hong Kong police say officers will wear unique identifiers as force defends recent treatment of journalists
- "Online Voter Information Enquiry System" (OVIES)

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/