Cybersecurity in Hong Kong – A Legal Perspective

Dominic Wai, Partner, ONC Lawyers

This presentation is not an exhaustive treatment of the area of law discussed and cannot be relied upon as legal advice. No responsibility for any loss occasioned to any person acting or refrain from acting as a result of the materials and contents of this presentation is accepted by ONC Lawyers.
Cybersecurity in Hong Kong – A Legal Perspective

• What is Cybersecurity?
• The Hong Kong Cybersecurity regime
• Criminal and Civil responses
• Law firms and legal aspects
• Cyber Risk Prevention and Protection
• Trends and challenges
• Q&A
Cybersecurity in Hong Kong – A Legal Perspective

- 29 April 2016 – FBI Warning
- Wireless Keystroke Logger disguised as USB Device charger targets wireless keyboards
- Criminals could steal – IP, Trade Secrets, Personally Identifiable Information (PII), Passwords, Other sensitive information
Cybersecurity?
What is Cybersecurity?

• Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.

• “The collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users’ assets.” – Cybercrime Prevention Act of 2012
Wide Range of Cybercrimes

• Data and Money Theft
  • Hacking
  • Stealing/Espionage
  • Wipe out
  • Phishing and malware
  • Unauthorized disclosure
• Identity Theft and Fraud
  • Business Email Compromise/Business Email Scams (BEC/BES)
  • Credit card details and passwords
Wide Range of Cybercrimes

• Ransomware/Extortion/Hijacking (botnets)

• Sabotage
  • Distributed Denial of Service (DDos)
  • Advanced attacks (e.g. the Stuxnet virus)

• Bullying/hate speech/vandalism/stalking

• IP infringement
Wide Range of Cybercrimes

- Criminal organizations
  - Commoditization – hacking tools are easily purchased with support
  - There is a market for the information they steal
  - cross-border and multi-jurisdiction – difficult to find, locate and apprehend
- Nation states
- Activism – hacking groups
- Terrorists
Risks and Loss

- Financial Loss
  - Loss of Intellectual Property (confidential information and trade secrets)
  - Theft
  - Business disruption – loss of trust; loss of business opportunity
- Damage to reputation (repeated citation?)
Risks and Loss

• Exploitation – devices being hijacked

• Loss of HK$1.82 B in 2015; 50% increase than 2014.
Risks and Loss

- Time and costs incurred on dealing with investigations
  - LEAs
  - Regulators – e.g. privacy commission – duty to notify or report the breach?
- Regulatory sanction
- Claims
  - By victims and 3rd parties
  - Liability to counterparty (persisting payment duty; contractual obligations)
- Multiplicity – incidents, areas, jurisdictions
Risks and Loss

- Outside (Technology)
  - Hackers
  - 3rd party and outsourcing
  - Cloud
  - Security weak websites

- Inside (People & Process)
  - Inadvertence/System Glitch/Human Error – unaware and unrecognized vulnerabilities
  - Rogue/disgruntled employees and insider

- Outside/Inside
  - BYOD – where is your endpoint?
  - Free Wi-Fi
The Hong Kong Cybersecurity regime

• Maintaining technological investigative capabilities
• Close cooperation with overseas LEAs and regulators, and HK Government departments and major stakeholders
• Raising public awareness on prevention
The Hong Kong Cybersecurity regime

• Office of the Government Chief Information Officer (OGCIO)(GOV:ITB)
  • Cyber Security Information Portal (CSIP)
  • www.cybersecurity.hk
• Police – Cyber Security and Technology Crime Bureau (CSTCB)(GOV:SB)
• CED – Electronic Crime Investigation Centre
The Hong Kong Cybersecurity regime

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)(HKPC)(Statutory Body)
- Centre for coordination of computer security incident response for local enterprises and internet users.
The Hong Kong Cybersecurity regime

• Office of the Privacy Commissioner for Personal Data (GOV:CMAB)
• Securities and Futures Commission (SFC)
• Hong Kong Monetary Authority
  • 2016 – Cybersecurity Fortification Initiative – raise awareness of cybersecurity within Hong Kong financial institutions through a 3-pronged approach:
The Hong Kong Cybersecurity regime

- CFI
  - Cyber Resilience Assessment Framework
  - Professional Development Programme
  - Cyber Intelligence Sharing Platform
The Hong Kong Cybersecurity regime

- Applied Science and Technology Research Institute (ASTRI)
- Government funded and Govt rep on the board.
- Cyber security summit 2016 and cyber security R&D – to enhance cyber security of Hong Kong and the region.
  - SecShare platform – cyber threat intelligence sharing platform.
Other Regimes

• Legislation
  • Singapore – Computer Misuse and Cybersecurity Act
  • Philippines – Cybercrime Prevention Act of 2012

• Authorities
  • Singapore – set up in 2015 - Cyber Security Agency (CSA) – reports to the PM’s office; oversee cyber security strategy, education and outreach, and industry development.
Other Regimes

- UK – setting up of the National Cyber Security Centre (NCSC) in Oct 2016.
  - Bring UK’s cyber expertise together to transform how the UK tackles cyber security issues.
  - Authoritative voice on information security.
  - Work with BOE to produce advice for the financial sector for managing cyber security effectively.
Criminal and Civil Responses

• Offences
  • “Unauthorised access to a computer by telecommunications” (s.27A of the Telecommunications Ordinance)(Cap 106)
  • “Access to a computer with criminal or dishonest intent” (s.161 of the Crimes Ordinance)(Cap 200)
  • “Disclosing Personal Data Obtained without consent from Data Users”
    • with an intent to obtain gain in money or other property, whether for the benefit of the person or another person; or
    • To cause loss in money or other property to the data subject. (s.64 of the PDPO)(Cap 486)
  • DPP4 – data users should take all practical steps to ensure that personal data held by the data user are protected against unauthorised or accidental access, processing, erasure, loss or use.
Criminal and Civil Responses

• Theft Ordinance (Cap 210):
  • Theft of Property (includes intangible property)(s.9)
  • Burglary (s.11(3A))—unlawfully causing a computer in the building to function other than as it has been established by or on behalf of its owner to function;
  • Unlawfully altering or erasing any program, or data, held in a computer in the building or in a computer storage medium in the building.
Criminal and Civil Responses

- Criminal damage – destroying or damaging property (Crimes Ordinance, ss 59(1A), 60(1))
- To destroy or damage any property in relation to a computer includes the misuse of a computer.
- Misuse of a computer –
  - To cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
  - To alter or erase any program or data held in a computer or in a computer storage medium;
  - To add any program or data to the contents of a computer or of a computer storage medium.

And any act which contributes towards causing the misuse of a computer as described above shall be regarded as causing it.
Criminal and Civil Responses

• But no definition of a computer in the relevant ordinances.

• Recent cases ruled mobile phones and smartphones are “computers” under s.161 of Crimes Ordinance.

• Meaning of “computer” – s.22A of Evidence Ordinance (Cap 8) – documentary evidence from computer records

  • “Any device for storing, processing or retrieving information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process.”
Criminal and Civil Responses

“Computer” means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

(a) an automated typewriter or typesetter;
(b) a portable hand-held calculator;
(c) a similar device which is non-programmable or which does not contain any data storage facility; or
(d) such other device as the Minister may, by notification in the Gazette, prescribe”
Criminal and Civil Responses

“Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device.

It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.”
Criminal and Civil Responses

• Police investigation
  • CED for Copyright Ordinance against providing device or services for “jail breaking” s.273C(1)(d)(Cap 528)

• Online report of cybercrime

• Interpol - Global Complex for Innovation (Singapore)

• Mutual Legal assistance on criminal matters

• The relevant ordinances on cybercrime mainly are not extraterritorial.
  • Save for CJO (Cap 461) for Theft
Criminal and Civil Responses

- Breach of contract
  - Employment contract
  - Outsource agreement
  - User agreement
- Breach of confidence
- Misuse of private information
- Breach of confidentiality/fiduciary duty
- Trespass to chattel
- Conversion
- Economic tort of intentional infliction of harm by unlawful means
- Derivative actions
- Class action (other jurisdictions)
Criminal and Civil Responses

- Legal means to seek access or retrieve data
  - Norwich Pharmacal Orders
  - Anton Pillar Orders
  - Ex Parte relief – authorizing the detention, seizure or preservation of property
- 3rd Party Discovery
Criminal and Civil Responses

- Internal investigation
- Notification
- Legal privilege
- Insurance/Cyber insurance
  - First and Third party losses
Law firms and legal aspects

• Risk
  • Data
  • Confidential information
  • Business secrets
  • Money
  • System vulnerability
  • Lack of awareness and training
  • Client due diligence/conformity to international standards e.g. ISO, NIST etc.
  • Fiduciary duties
  • Professional duties
Cyber Risk Prevention and Protection

- Tech is pervasive and it’s only a matter of time that you will be hacked or disrupted in a bad way.
- It’s not just an IT issue – it’s people, process and tech.
- Everyone has a part to play and humans are the weakest link.
- Difficult to catch the culprits – they are anonymous, out of the jurisdiction and data and money moves at lightning speed.

- What can you do?
  - Raise awareness and training
  - Situational awareness – digital footprint - the Dark Web
  - Where are your jewels?
  - What are your weak points?
    - Risk assessment
    - Legacy systems – updates and upgrades
Cyber Risk Prevention and Protection

- Have a plan
  - Crisis management
  - Resilience
- Test and monitor – does the plan work and are people following policies.
- Vet – staff, service providers, cloud.
- Beware of Free Wi-Fi.
- Record/paper trail – responses, remedies and mitigation.
Cyber Risk Prevention and Protection

• Watch out for:
  • Phishing emails/Business email scams
  • Ransomware
Phishing Email

Good Morning

Please see attached outstanding invoice for the month of April 2016 due for payment. Kindly arrange payment as soon as possible without any delay.

Kind Regards

Andrew Lim

Hong Kong Bar Association
Address: 38 High Court of Hong Kong,
Queensway, Hong Kong Lower 2nd floor
Phone: +852 2869 0210
Phishing Email

- Emails (or other medium) pretending to be from a genuine source or someone you know to gain your trust and convince you to do something that benefits the fraudster.

- Spotting phishing:
  - Be suspicious
  - Does the communication make sense?
  - Ask you for confidential and private information like logins or passwords.
  - Ask you to open attachments or click on a hyperlink or visit some websites.
  - Check Message Headers – Email meta-data that includes message routing information.
  - Don’t “Reply”, “Forward” the email when replying if the email is suspicious.
  - Contact the person – call the person to verify.
Passwords

• **Strong Passwords:**
  • Use a combination of lowercase, uppercase, numbers, and special characters of 8 characters long or more like s9%w^8@t$i.
  • Use short passphrases with special characters separating to make it difficult for crackers and could be easily remembered like cry%like@me (cry like me).
  • Avoid using the same combination of passwords for different websites.
  • If it is difficult for you to remember different passwords for different websites, then use Password Manager applications like RoboForm, 1Password, LastPass.
Ransomware

- Advice from FBI
  - Implement a robust data back-up and recovery plan. Maintain copies of your files, particularly sensitive or proprietary data, in a separate secure location. Back-up copies of sensitive data should not be readily accessible from local networks i.e. store the back up offline.
  - Never open attachments included in unsolicited emails. Be very vigilant about links contained in emails, even if the link appears to be from someone you know. Go to the links DIRECTLY.
  - Keep your anti-virus software up to date.
  - Enable automated patches for your operating system and web browser.
  - Only download software, especially free software, from sites you know and trust.
  - Don’t pay the ransome (HKCERT advice too)
Trends and challenges

- Internet of Things (IoT)
- Automated cars
- Drones
- FinTech
- 4.1B people yet to be connected
Key takeaways

• Be vigilant – err on the side of caution
• Switch off your computers
• Never send confidential information to your personal email account
• Do not share password with others
• Never click suspicious link or attachments in an email
• It’s not about you – It’s about others – your loved ones, your friends, your firm/company
Cybersecurity in Hong Kong – A Legal Perspective

Q&A
solutions • not complications