ONC Lawyers

柯伍陳律師事務所

Role of the Board and Directors in Tackling Cybersecurity and Fintech issues

Dominic Wai, Partner, ONC Lawyers

11 July 2017

CHKLC training Series

ONC Lawyers

Content

- Case Studies
- Types of Cyber Risks facing companies in Hong Kong
- Role of the Board and Directors' duties with respect to cybersecurity
- Criminal and Civil Responses
- Cyber risk prevention and protection

ONC Lawyers

- 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

ONC Lawyers

Cybersecurity in Hong Kong

- Who is liable?
- Who put it there or bring it in?
- What is the company's policy on that?
- Was it deliberate or due to inadvertence?
- Is it pursuable or worth pursuing?
- Do we need to report or notify anyone or any institutions?
- Do we have insurance to cover this?

ONC Lawyers

Case Study I

- P is an overseas company; D1 and D2 are HK companies.
- Ms D is an employee of S, P's parent company.
- Ms D works in the accounts dept as a **temporary administrative assistant**. She is responsible for processing payments to P's various suppliers, as well as other administrative tasks. She has been with S for 6 months.
- In Nov 2015, Ms D received various emails from a person purporting to be a Mr A, a director of P and Chairman of its board of directors. The emails described Mr A as "CEO" of P and were sent from an email address, g.a@mail.com (but spoofed to look like the real email address of Mr A)
- Mr A is not the CEO of P and g.a@mail.com is not Mr A's email address.
- The emails from the "CEO" asked Ms D to contact a law firm allegedly acting for P in relation to an alleged purchase of a company. Ms D was instructed to email a Mr M, the alleged lawyer, at another email address: c-j-k@consultant.com.

ONC Lawyers

Case Study I

- Ms D was also advised that the alleged transaction was highly confidential and that she must not inform anyone else of it. Mr A instructed Ms D to communicate with him by email only.
- On the same day, Ms D received a telephone call and various emails from Mr M (the “lawyer”). The emails identified Mr M as “C J K, lawyers – specialist in tax law, lawyers – specialist in company law”. The emails also included a logo for “C J K, lawyers”.
- Mr A and Mr M together instructed Ms D to make an express transfer of USD 400,000 from P’s bank account to a bank account with a bank in HK. The beneficiary of that account was D1, a trade company.
- Following receipt of these instructions, Ms D contacted P’s bank and arrange the funds to be transferred from overseas to HK. After the transfer had completed on **26 Nov 2015**, Ms D forwarded the confirmation of the transfer to Mr A.

ONC Lawyers

Case Study I

- On **30 Nov 2015** a manager of the accounts dept and chief executive officer of S noticed that USD 400K had been debited from P's bank account. She then asked Ms D about the transfer. The manager then raised this transfer with (the real) Mr A and Mr A confirmed that he was unaware of the transfer and had not sent the emails.
- The matter was reported to the Overseas and HK Police on 1 Dec. On Feb 2016 the HK Police confirmed that D1's bank account had been "frozen". Some money was transferred from D1's account to D2's account and that account had also been "frozen". The combined monies were at least USD 400K.
- According to P, its online arrangement with the Overseas bank does not authorize international transfers.

ONC Lawyers

Case Study I

- Issues
  - Bank would not disclose who was D2 (some funds were transferred from D1 to D2)
- Finding D2
  - Information disclosure order – Norwich Pharmacal Order – discovery against non-parties (bank) before start of proceedings
  - A Norwich Pharmacal Order will not be made in cases involving considerable administrative inconvenience
  - Costs paid by the party seeking the Order
  - In this case, the Order required the bank to provide certain documents concerning D2 such as the account numbers of D2's account and confirm the balance of the accounts.
- Injunction
  - Restraining Ds from removing or disposing of assets

ONC Lawyers

Case Study I

- Claims
  - Damages
  - Unjust Enrichment – declaration that Ds have been unjustly enriched and account to the Plaintiff for the unjust enrichment
  - Declaration that certain sum was the property of the Plaintiff and was received and held by Ds as constructive trustee
  - Order that the balance of Ds' accounts be paid to the Plaintiff
- Sue and obtain judgment
- Enforcement of judgment
  - Garnishee order – apply for an order for the bank to pay the bank account balance to the Plaintiff to satisfy the judgment
  - Beware of competing claims and enforcement applications
- Criminal investigation
  - Can continue
  - If convicted, Court might grant a restitution order.

ONC Lawyers

Case Study I

"In 2017, we predict that BEC will remain a prominent threat and will be used in more targeted scams" – Trend Micro

BEC scams typically use subject lines that imply urgency regarding payments inquiries or fund transfers such as:

- Payment – Important
- Payment Notice
- Process Payment
- Quick Request
- Fund Repayment Reminder
- Wire Transfer Request
- Bank Transfer Enquiry

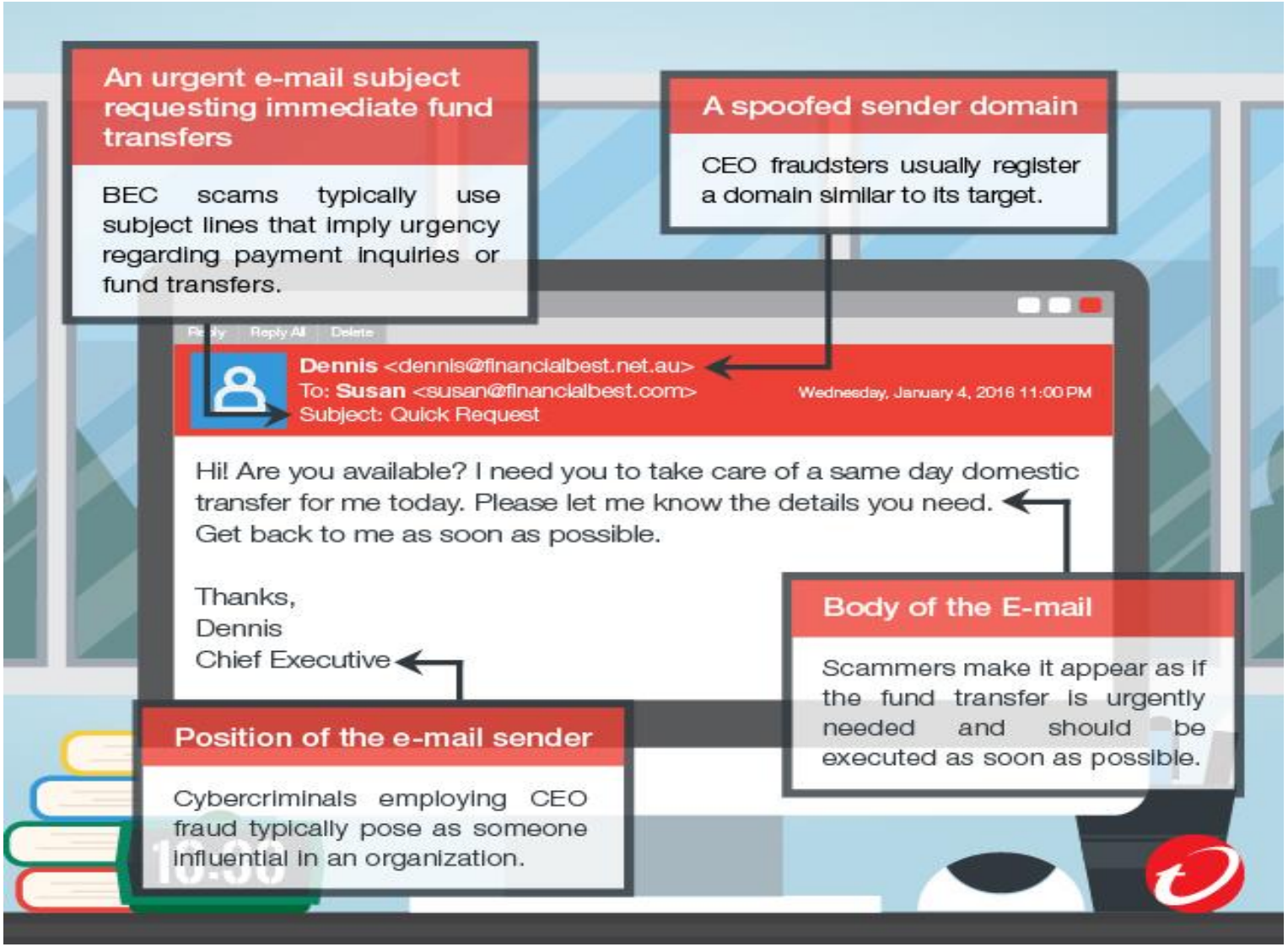
ONC Lawyers

Business Email Compromise (BEC)

Surveillance of target company	Identify key individuals	Fraudulent email requesting transfer	Pressure emails	Transfer to fraudster's account	Further requests
• Public Information • Inside Information (hacked) • Phishing Emails	• CEO • CFO • Financial Controller	• Appears legitimate • From similar address • From hacked account • Timing	• Further email exchanges with imposter	• Overseas account • Money moved again (hard to trace)	• Often successful • Not worried about being caught

"John, our longtime supplier BestCo is having tax re-structuring issues **and wants us to make this month's payment to a different account**. Can you please arrange urgently. I'm attaching the remittance instructions."

ONC Lawyers



- Source: Trend Micro, Jan 2017

ONC Lawyers

What is the cybersecurity outlook of Hong Kong?

- Hong Kong Police
  - The world is exposed to much higher risks of cyber security threats
  - In 2016, there were a number of high-profile cyber attacks targeting financial institutions and critical infrastructures (e.g. SWIFT hacked – USD81M to Bangladesh Central Bank; Ukarine power grid hacked causing blackout in Dec 2015 affecting a million people)
  - The industry control systems installed by power plants in HK could be the next target.
  - Corporate Email Scam (867 no of cases -2016)

ONC Lawyers

What is the cybersecurity outlook of Hong Kong?

- Symantec 2016 Internet Security Threat Report indicated that HK had climbed from 8th to 7th place in the regional threat ranking for Asia Pacific.
- It was reported that the number of DDos attacks increased 43% to more than 34,000 attacks in the APAC region in the first half of 2016, and the largest increase was observed in HK accounting for a 57% rise in attacks.
- Cyber security experts predicted that malware attack against mobile phones and Internet of Things (IoT) such as webcams, smart TVs etc would witness an upsurge and create a huge concern on cyber security.
- Hong Kong Computer Emergency Response Team (HKCERT) received 4,928 cyber security incident reports in 2015, representing a 500% increase since 2010.

ONC Lawyers

What is the cybersecurity outlook of Hong Kong?

- In Hong Kong, the annual number of local reports of technology crimes has increased significantly by 24 times from 272 cases in 2002 to 6,862 in 2015. In 2016 (as at September), the number of cases has already hit 4,537.
- Over the past six years, the respective annual financial losses have also increased by 30 times from $60 million in 2010 to $1.8 billion in 2015.
- In 2016 (as at September), the loss is around $1.87 billion.

ONC Lawyers

Case Study II - 2016

- P is a HK company engaged in the trading of securities, options and futures contracts, and investment holding.
- D is a corporation licensed to carry on Type 1 (dealing in securities) regulated activities under SFO (Cap 571) and also an Exchange Participant of the Stock Exchange of Hong Kong Limited and Hong Kong Futures Exchange Limited.
- P has a securities account with D that can be operated online with the use of specified user ID and password for online access to the account for the purpose of carrying out transactions for the sale and purchase of securities. According to P, there are only 3 persons in the company who are authorized to access and operate the account with D and conduct online securities transactions with the account.

ONC Lawyers

Case Study II - 2016

- On 23 Sept 2016, between 14:40 and 15:22, unauthorized person(s) logged into P's account with D with a valid user ID and password from an IP address and in the space of 18 minutes, bought a total of 49.2m shares in a Listco from a total of 76 selling brokers at a purchase cost of HK$37.69m (including fees and levies), draining almost all of the HK$37.85m cash in the account.
- The 49.2m shares represent 4.92% of the Listco's shareholding at an average price of HK$0.7636 per share, 36% above the previous day's close.
- There was a huge spike in the volume and price of the Listco on 23 Sept 2016: the traded volume was 92.568m shares or 9.26% of the ListCo and the price at one point reached HK$0.88, up 57.1% on the previous close of HK$0.56, before closing at HK$0.66, up 17.9%.

Source: Webb-site.com

ONC Lawyers

Case Study II - 2016

- On 23 Sept 2016 at around 16:24, P was first alerted by D of the transactions.
- P then carried out some internal investigation and at around 16:47 on the same day informed D that the transactions were unauthorized.
- P's case was that the transactions were unauthorized and were carried out fraudulently by a "hacker" who somehow gained access to P's account through D's online banking system.
- P refers to the fact that the records of D's online trading system show that the person(s) who logged into the account between 14:40 to 15:22 on 23 September 2016 did so from a device with an internet protocol address (IP address) different from the IP address(es) of the device(s) normally used by P to access the account.
- SFC announced that in the last 12 months there have been 16 incidents involving 7 brokers and total unauthorized trades in excess of HK$100m. The cases are under police investigation.

ONC Lawyers

Case Study II - 2016

Recourse

- Injunction
  - Order for completion and settlement of the share transactions be withheld and/or suspended until further order of the Court
  - Test
    - There is a serious question to be tried (the claim is not frivolous or vexatious)
    - The balance of convenience lies in favour of granting an injunction
  - Documentation
    - Affidavit – setting out the facts in support of the application. Ex parte application – duty of full and frank disclosure of all material facts

ONC Lawyers

Case Study II - 2016

"If you ask regulators in the industry what is the number one threat, not surprisingly it’s all about cyber attacks," "We've seen that happen not only in banking but also at brokers in Hong Kong, in particular recent attacks to do with basically hijacking share trading accounts."

- Ashley Alder, CEO of the SFC and chairman of the International Organization of Securities Commissions, said in a speech to the local legislature last week – Reuters, Feb 2017

HKMA suggests 2 factor authentication – not mandatory requirement in HK

HKAB survey – not favourable – fear that it would affect the volume and speed of transactions.

ONC Lawyers

Wide Range of Cybercrimes

- Ransomware/Extortion/Hijacking (botnets)
- Sabotage
  - Distributed Denial of Service (DDos)
  - Advanced attacks (e.g. the Stuxnet virus)

ONC Lawyers

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

ONC Lawyers

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

ONC Lawyers

Role of the Board and Directors' duties

- In general, the directors have the duty to act for the best interest of their company and liability may arise from the breach of such duty.

- Civil suits may be brought by the shareholders, customers or even employees against the directors of the companies attacked.

ONC Lawyers

Role of the Board and Directors' duties

Reasonable Care, Skill and Diligence

- Common law duty
- Codified in Companies Ordinance (s.465, Cap 622) – owed to the company
- What is "reasonable"?
  - Assessed against the knowledge, skill and experience that one would reasonably expect a Hong Kong company director to have
- Failure to meet standard
  - Director's liability

ONC Lawyers

Role of the Board and Directors' duties

Failure to manage cyber risk leading to cyber attacks– could be a breach of duty, negligence and mismanagement

- Grounds for derivative actions (s.731)
- Minority shareholder action – unfair prejudicial conduct (s.724)

Listed companies - if the business or affairs of the company have been conducted

- in a manner involving misfeasance (negligence) or other misconduct towards the company or its members or
- Unfairly prejudicial to its members

ONC Lawyers

Role of the Board and Directors' duties

SFC may petition to the Court for an order that may include (s.214 of Securities and Futures Ordinance, Cap 571):

- Appointing a receiver or manager to manage the Listco
- Order that a person shall not, without the leave of the Court, be or continue to be a director of the company or take part in its management

ONC Lawyers

Role of the Board and Directors' duties

Rule 3.08 of the Listing Rules:

A director is responsible for fulfilling his duties of skill, care and diligence to a standard at least commensurate with the standard established by Hong Kong law and was further required to, inter alia, apply such degree of skill, care and diligence as may be reasonably expected of a person of his knowledge and experience and holding his office within the company.

A director is required to follow up anything untoward that comes to his attention.

ONC Lawyers

Role of the Board and Directors' duties

Example U.S. Case – Sony

- In Nov 2014, Sony's information technology infrastructure and network were hacked as a result of inadequate security measures.

- About 100 terabytes of data were stolen from the system, which include sensitive personal information of the former Sony employees.

- In March 2015, nine employees filed a class action in California against Sony, claiming that Sony had been negligent and had breached implied contract.

ONC Lawyers

Role of the Board and Directors' duties

Hong Kong Cases

- No class action has yet been brought in Hong Kong against companies attacked and the majority of cases took place in the U.S.

- But similar legal basis, such as negligence, is also available in Hong Kong. Therefore, HK companies are not immune.

ONC Lawyers

Role of the Board and Directors' duties

UK – ICSA Guidance Note on Cyber Risk

- The cyber threats facing businesses and their supply chains cannot be prevented through investment in technology alone.
- Boards, with the assistance of the audit committee, should provide ultimate oversight of strategic and operational cyber risks, as they do other key risks.

ONC Lawyers

Role of the Board and Directors' duties

Boards might find it helpful to focus on the following points:

- Understand your company's cyber risk. It is very specific to an individual organization's situation, even within a single market sector.
- Make an active decision as to the balance between the risk the organization is prepared to take, and the costs to be incurred in targeted spending, to protect the organization from cyber attack.
- Plan for resilience. As threats become more sophisticated, focus on resilience to attacks that get through, rather than preventing all cyber attacks.
- Be clear who is responsible for owning the risk, allowing for the dynamic and sometimes targeted nature of a cyber threat. Boards may consider giving one director specific responsibility for oversight of cyber risk.

Source: ICSA Guidance Note on Cyber Risk

ONC Lawyers

Role of the Board and Directors' duties

Boards may wish to ask management these questions:

i. How confident are we that our company's most important information is being properly managed, and is safe from cyber threats?

ii. Are we clear that the board's directors could be key targets?

iii. Do we have a full and accurate picture of:

   i. The impact on our company's reputation, share price or future survival, if sensitive internal or customer information held by the company were to be lost or stolen;

   ii. The impact on the business if our online services were disrupted for a short or sustained period?

ONC Lawyers

Role of the Board and Directors' duties

Exploring who might compromise our information and why it is critical

i. Do we receive regular intelligence from the Chief Risk Officer (or equivalent) on who may be targeting our company, their methods and their motivations?

ii. Do we encourage our technical staff to enter into information-sharing exchanges with other companies in our sector and/or across the economy, in order to benchmark, learn from others and help identify emerging threats?

ONC Lawyers

Role of the Board and Directors' duties

Pro-active management of the cyber risk is critical

i. Cyber risk potentially impacts share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology, and finance. Are we confident that:
   - We have identified our key information, and thoroughly assessed its vulnerability to attack;
   - Responsibility for cyber risk has been allocated appropriately on the risk register;
   - We have a written information security policy in place, which is championed by us and supported through regular staff training;
   - The entire workforce understands and follows the policy.

Role of the Board and Directors' duties

Do we understand the consequences of failure:

i. To the company's financial stability;
ii. To the company's brand and reputation;
iii. To the company's future strategy; and
iv. To the potential for corporate failure?

ONC Lawyers

Role of the Board and Directors' duties

What is expected of the board:

- Responsibility of protecting the company's critical assets including sensitive information of its customers and to play a PROACTIVE ROLE in ensuring effective cybersecurity risk management:
  - Risk ownership and management accountability – strong security awareness and culture across a full spectrum of users (management, staff/contractors and service providers)
  - Periodic evaluations and monitoring of cybersecurity controls
  - Contingency planning
  - Regular independent assessment and tests

Source: Circular on Cyber Security Risk Management, HKMA, 15 Sept 2015

ONC Lawyers

Role of the Board and Directors' duties

But not easy to achieve – why?

- Vulnerability – hardware, software (programs, web browsers etc)
- Don't know where the threats/attacks are coming from - you can't protect things that you cannot see.
- Terms and concepts that are not easy to understand
  - "Malware"
  - "Phishing"
  - "Cloud"
  - "Social Engineering"
  - "Vectors"

ONC Lawyers

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.

ONC Lawyers

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.

ONC Lawyers

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.”

ONC Lawyers

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

ONC Lawyers

Criminal and Civil Responses

- **Law Enforcement**

- Companies should maintain a close connection with various law enforcement representatives to discuss before an incident occurs:

”

  - When should the company report the incident to them.

  - How the reporting should be performed.

  - What evidence is needed.

  - How evidence should be collected.

ONC Lawyers

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

ONC Lawyers

Criminal and Civil Responses

X needs to pay A under a contract. A fraudster, B, by BEC pretended to be A and requested X to pay B instead. X paid B accordingly. A chased X for payment under the contract as A had not been paid.

Does X need to pay A?

Will a Force majeure clause help?

ONC Lawyers

Criminal and Civil Responses

- Where a force majeure clause is included in a contract, the precise language of the clause will determine the enforceability of the contract and the parties' obligations thereunder if certain uncontrollable outside events: a "force majeure" prevents performance.
- Parties can expressly provide that the risk of supervening events shall be borne by one of them and not the other or they can apportion it or deal with it in various other ways.
- Accordingly, contracting parties are well-advised to consider their cybersecurity risks when drafting contracts, including the insertion of suitably worded force majeure clauses.

Criminal and Civil Responses

- Legal means to seek access or retrieve data
  - 3rd party disclosure orders
  - Anton Pillar Orders
  - Ex Parte relief – authorizing the detention, seizure or preservation of property
  - 3rd Party Discovery

ONC Lawyers

Criminal and Civil Responses

- Internal investigation
- Notification
- Legal privilege
- Insurance/Cyber insurance

ONC Lawyers

Criminal and Civil Reponses

- Consider buying cyber insurance (but do not ignore IT security)
- 3rd party claims
  - Claims for compensation, investigations, payment of fines and penalties. Also cover defence costs and legal representation expenses.
- Business Interruption
  - Reimbursement for lost profits
  - Necessary expenses incurred to maintain operation of the business as a result of the interruption.

ONC Lawyers

Cyber risk prevention and protection

- **Initial Response to Cyber Attack**
  - Questions that the board and management should be asking:
    - Was data stolen?
    - How does it impact our business?
    - Who did that?
    - How did they get in?
    - How much access did they have?
    - How do we remove it?
    - How do we prevent it from happening again?

ONC Lawyers

Takeaways - 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)
  - **Beware of email/online HR applications.- malware download**

ONC Lawyers

Takeaways - Tips to protect from BEC

- Always verify, especially when it comes to messages that involve fund transfers.
  - Emails accounts might have been hacked and compromised already – need protocols that include verification other than email. – phone, text messaging, chat apps
  - Don’t “Reply”, “Forward” the email when replying if the email is suspicious. This is to ensure that you are not replying to a spoofed address.
  - Have a mail security solutions in place that will check for dangerous attachments and also social engineering correlations.

Source: FBI and Trend Micro

ONC Lawyers

Takeaways

- 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.
  - Not a dictionary word or combination of dictionary words – “House” “Red House” “H0use”

ONC Lawyers

Takeaways

Resources

- Cyber security information portal (CSIP)
  - http://www.cybersecurity.hk/en/index.php
- HKCERT
  - https://www.hkcert.org/incident-reporting;jsessionid=97030B274CB0B3D8193B949A8275986C
- Hong Kong Police e-report room – report of cyber crime
  - https://secure1.info.gov.hk/police/eforms/report_cyber_crime_en.php
- Cybersecurity ratings – benchmarking business partners and vendors
- International standards
  - ISO 27000 family of standards on Information technology

ONC Lawyers

THANK YOU

ONC Lawyers

Dominic Wai
Partner of ONC Lawyers
19/F., Three Exchange Square,
8 Connaught Place, Central, Hong Kong.
Tel.: 3906 9649 Fax : 2804 6311
Email : dominic.wai@onc.hk

ONC Lawyers

solutions • not complications