RAJAH & TANN | *Myanmar*

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

COVID-19 AND CYBERSECURITY RISKS

Legal Strategies for Businesses in Myanmar

4 May 2020

Chester Toh, Co-Head of Myanmar Practice

CAMBODIA | CHINA | INDONESIA | LAO PDR | MALAYSIA | MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM

Current Regime on Cybersecurity

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Myanmar Government has been developing a dedicated cyber law since 2018. Currently responsible department is Information Technology & Cyber Security Department under MoTC. Established a National Cyber Security Centre
- Currently only laws regulating cyber crimes in the country. Enforcement is fraught with challenges as many of the perpetrators are based overseas. Also no centralised dedicated reporting system. Courts and judges ill-equipped to handle cybercrime cases
  - Section 34 of Electronic Transactions Law
  - Section 66 of Telecommunications Law
- No omnibus data protection or privacy law also meant that many companies do not have policies to handle and secure personal data. Generally little awareness that personal data requires special handling
- 2005-2010 ICT Master Plan – Cybersecurity Protection Agency
  - *Prevent cyber-attacks against Myanmar's critical infrastructure*
  - *Reduce national vulnerability to cyber-attacks*
  - *Minimise damage and recovery time from cyber-attacks*
- 2015 e-Governance ICT Master Plan – proposed Cyber Security & Investigation Committee under ICT Council reporting to President's Office

Current Regime on Cybersecurity

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Cybersecurity awareness and spending remain low notwithstanding sharp increase in number of mobile phone and internet users following opening up of Myanmar and liberalisation of telecommunications sector
- Within public sector, many government agencies do not have a dedicated cybersecurity unit, let alone cyber-breach response policies
- No formal critical infrastructure designation – concept probably not well understood within public service. Requires a nation-wide risk assessment
- As Myanmar embarks on more digital e-government services eg. MyCo, new IP registration system, the country requires a cohesive and effective cyber defence strategy
- mmCERT (Myanmar Computer Emergency Response Team) – non-profit organisation funded by the Myanmar Government:
  - handle cybersecurity incidents
  - engaged in providing technical advisory support
  - coordinate efforts and cooperate with law enforcement agencies on cybercrime and information security issues
  - promoting public awareness

Myanmar Environment Presents Cybersecurity Nightmare for Businesses

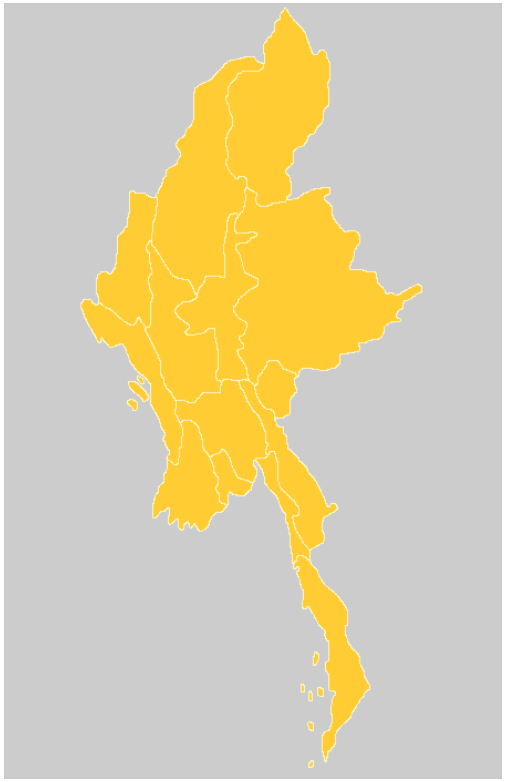
RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- A number of foreign businesses have only recently established small operations in Myanmar – lack resources and investments on cybersecurity and associated training
- Limited market for encryption technologies and cybersecurity solutions even if one is prepared to invest
- No cybercrime insurance products in local market
- Internet speed and bandwidth limitations make remote supervision/access difficult
- Use of unlicensed software in Myanmar continues to be prevalent
- Yet increasingly, more services are introduced online eg. e-banking, mobile money. Myanmar businesses often excited by what technology brings without correspondingly investing in cybersecurity
- Work from home arrangements are not common, not many employees provided with company issued laptops, especially junior staff
- Managers often lack experience in handling cybersecurity or data breaches. No breach notification requirements could lead to cover ups or companies electing not to announce for fear of reputational repercussions

Risks Faced by Businesses in Myanmar

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Low awareness of need to secure and protect online activities, eg. weak passwords set by users
- For Myanmar companies, transitioning from filing cabinets to online databases requires a mindset shift
- No incident response plan in place or plans that are not adapted/tailored to local circumstances in the case of foreign companies
- Weak economic environment in Myanmar for past few years meant companies are keeping a tight watch on costs, little budget allocated for vulnerability assessments and penetration testing which are perceived as “nice-to-haves”. Solutions providers are primarily foreign and not always cost effective



A case study in point

- June 2015, an employee of Ooredoo in Mandalay passed the call log of a customer in Yangon to a friend who in turn gave it to the customer's business associate
- The ex-employee in question accessed Ooredoo's customer relationship management system as she worked in the customer experience department of the telco's Mandalay office
- Customer reportedly engaged a lawyer but ultimately did not pursue legal action against Ooredoo
- Ooredoo however terminated the employee in July 2015
- Police report was reportedly made by Ooredoo
- Unclear if the company took any civil action

Responsibility as Business Leaders

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- In midst of Covid-19, business leaders often struggle with striking the right balance between:
  - Keeping business operations going
  - Keeping employees safe and maintaining staff morale
  - Ensuring continued proper supervision and oversight
- At the onset of Covid-19 pandemic, businesses were struggling with:
  - Keeping up to date with Government directives and restrictions in Myanmar
  - Managing concerns of local employees who were nervous over low official counts and rumours circulating online or via social media
  - Addressing concerns of foreign employees with Myanmar's healthcare system, Thingyan break and increasing flight cuts
  - Practical difficulties of implementing WFH arrangement in Myanmar
    - Internet bandwidth and difficulties procuring laptops of appropriate specifications at short notice
    - Limited training and experience with WFH
    - Many processes still operate in physical world, still document-heavy
    - Supervision challenging if foreign managers are supervising from afar, having left the country and not allowed back due to no-fly restrictions
- Businesses especially vulnerable to cybersecurity threats during this Covid-19 pandemic

Responsibility as Business Leaders

Implementation of WFH at short notice: forced into a corner, would convenience triumph? eg. security tokens issued by banks for online banking, employee personal devices etc.

- Cybersecurity risks and directors duties?
  - Myanmar Companies Law
  - Myanmar common law which encompasses case law
  - Company's Constitution
  - Other statutory duties
  - Stock exchange rules in cases of listed companies
- MCL: sections 165 to 172 (not exhaustive). Primarily fiduciary duties and obligations – duty to act with care and diligence, act in good faith in company's best interests and avoid conflicts of interest etc.
- Other common law duties include duties of confidence
- What does it all mean?! Can I delegate it to someone with the expertise?

Responsibility as Business Leaders

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Board is responsible for, amongst others, oversight and risk
- Increasing number of cyber-attacks globally even before Covid-19 meant that cybersecurity risk is as significant as other risks such as operational, financial, compliance risks

→Board has a duty to oversee the company's management and response to cybersecurity risks

- Myanmar has been subjected to a number of cyber-attacks over the years, no excuse for turning a blind eye
- Key steps to take:
  - Understanding cybersecurity risk and what is means from a supervisory / oversight perspective
  - Identify who is best placed to manage cybersecurity risks having regard to company size, industry (whether potentially a CI even in absence of government designation), existing risk management framework. For example, is there already a DPO covering Myanmar even if such person may be outside of the country?
  - Put off by technical jargon from IT or your vendors? You are not alone! There is a need to crystallise a succinct, accessible "plain English" cybersecurity governance plan

Responsibility as Business Leaders

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Key steps to take (cont'd):
  - Risk-based approach – secure most vulnerable information assets and systems as well as "crown jewels" but have adequate base-line perimeter fencing for less sophisticated attacks
  - Limited resources may mean one has to prioritise risks – look to capture know-how in terms of the sort of cyber risks that the company has encountered and are witnessing on an ongoing basis
  - Importantly, recognise that it's not a matter of "if" but rather "when" the company will be attacked → develop an incidence response plan
  - Update risk prioritisation matrix, incidence response plan and also keep abreast of latest developments, eg. emergence of ransomware as well as latest cybersecurity tools/technologies, best practices, legal obligations etc.
  - Addressing employee lapses – a culture of accountability and cross-functional collaboration is required. Ongoing training and crucially, right "tone from the top"

→ It will take you outside of your comfort zone but truth is, there is no better time given the heightened risks and seeing first hand the actual challenges that Covid-19 pandemic has posed to our ways of working

Practical Steps to Take

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Delegate? Section 160 of MCL allows the board to delegate any of its powers to a committee of directors, a particular director, an employee or any other person (eg. third party vendor) provided that the company's Constitution permits such delegation
- If directors choose to delegate, directors responsible for the exercise of the power by the delegate as if the power had been exercised by the directors themselves unless they can show that they reasonably believed that:
  - at all times, the delegate would exercise the power in conformity with the duties imposed on the directors by MCL and the company's Constitution; AND
  - in good faith and after making proper inquiry (if the circumstances indicated the need for inquiry) that the delegate was reliable and competent in relation to the power delegated

  → fine to utilise experts but one must make sure that experts can do the job!

Practical Steps to Take

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

5 Steps Plan

- Map out the core assets, risks faced by organisation, priorities and responsible parties
- Implement safeguards to prevent intrusions, institute access controls, encryption etc. Start putting in place cybersecurity awareness and training. Educate staff on social media use especially in times of stress – irrational behaviour cannot be discounted
- Ensure timely detection of cybersecurity breach with continuous security monitoring. Look out for digital behavioural indicators, eg. unusual log-in times and frequency
- Integrate breach response plan into your company's crisis management framework. Line up experienced specialist advisors to help guide company through a cybersecurity breach
- Develop post-incident recovery plans to resume business activities, plug any gaps identified and incorporate lessons learnt accordingly

Final Observations

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

- Covid-19 will ultimately go away but cybersecurity risks are here to stay
- Unlike a vaccine, there is no way one can be immune from cyber attacks
- Myanmar's CERP (27 April 2020) – *Goal 5: Promoting Innovative Products & Platforms.* Silent on the issue of cybersecurity and cyber-resilience – corresponding investments required
- Will we see a wave of cyber-attacks in the lead up to the general elections this year?
- Development of a comprehensive cybersecurity regulatory regime will take time. Companies cannot use absence of legislation as an excuse for inaction
- Inherent challenges in Myanmar – road will be long and hard but businesses need to take the first step

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

THANK YOU

Rajah & Tann Myanmar Company Limited
Myanmar Centre Tower 1, Floor 07, Unit 08,
192 Kaba Aye Pagoda Road, Bahan Township
Yangon, Myanmar

+951 9345 343 / +951 9345 346

Info@rajahtannasia.com

mm.rajahtannasia.com

Speaker Profile

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

Chester Toh

Partner, Rajah & Tann Singapore LLP
Director, Rajah & Tann Myanmar Company Limited

E chester.toh@rajahtann.com
T +65 6232 0220

LLB (Hons), National University of Singapore
Advocate & Solicitor, Supreme Court of Singapore

With a wealth of experience having practised in London, Hong Kong, Beijing and Singapore, Chester is uniquely placed to advise international clients on their ventures into new markets such as Myanmar. As co-head of our Myanmar Practice, he has advised numerous multinational companies and Asian companies in their investments into this frontier economy. He has been closely involved in a number of landmark transactions and projects in the country. At the same time, Chester heads up the Firm's Integrated Regulatory Practice. Clients routinely turn to him for regulatory risk assessment when investing in developing economies.

A recognised expert on FDI into Myanmar, Chester is regularly cited in publications and the media on Myanmar. He has spoken at numerous conferences on a range of topics relating to the country and is rated in leading legal journals such as Chambers Asia Pacific, Legal 500, AsiaLaw and IFLR. Chester also maintains a very active regulatory practice in the areas of telecommunications, media, data privacy and antitrust.