BDO

BDO CONNECT

Protecting Your Data Security and Data Privacy
Page 4 to 7

How CorpPass Affect Businesses
Page 8 to 9

From OJEK to GO-JEK: Internationalisation may not be as far-fetched as you think
Page 10 to 12

MANAGING PARTNER'S MESSAGE

Frankie Chia
BDO Singapore

The SingHealth data breach incidence is a timely reminder that cyber threats are real and can happen to any organisations. With ongoing investigations into the case revealed more insights that we can take lessons from it. If you who have been following and reading our newsletters and articles published recently, you would have noticed that we have been focusing on the subject. We believed cybersecurity is critical given our business eco-system. With businesses push towards digitalisation to drive efficiency, we cannot afford to ignore or take cybersecurity considerations lightly. During the October Cybersecurity Awareness Month, we published news bites and articles to raise awareness on the subject. We hope you have the time to read them and benefitted from it. In this issue, we are pleased to include two thought pieces that we hope will help you.

We are also pleased to inform you that BDO in Singapore is now a Council for Registered Ethical Security Testers (CREST) accredited firm for penetration testing services, an assurance that we are a trusted firm with quality and technical expertise to deliver quality, value-added penetration testing services. Currently, we are the only mid-tier professional firm in Singapore that is accredited. I encouraged you to speak to our cybersecurity team if you want to learn more about how we can help you to beef up your cybersecurity readiness.

Have a good read and enjoy!

CONTENTS

Understanding of Personal Data Protection Act (PDPA) and determination of PDPA impact to my business

What is PDPA?

Personal data refers to data, about an individual which can be used to identify that individual; or from that data and other information to which the organisation has or is likely to have access. Personal data in Singapore is protected under the **Personal Data Protection Act 2012 (PDPA)**.

The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

The PDPA also provides for the establishment of a national Do Not Call (DNC) Registry. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations.

How does PDPA impact any organisation?

As an organisation, personal information of employees, suppliers and/or customers are handled in it's daily activities and all these information handled by the organisation falls under the governance of PDPA for the collection, use, disclosure and care of the data. Under PDPA, organisations are required to develop and implement policies and practices that are necessary to meet its obligations under the PDPA.

In particular, organisations are required to designate at least one individual, known as the data protection officer (DPO), to oversee the data protection responsibilities within the organisation and ensure compliance with the PDPA.

Non-compliance of the PDPA can result in an enforcement notice preventing an organisation from processing data, effectively preventing an organisation from operating, together with significant fines. Furthermore, the officers of the organisation, the managers and directors, can be held personally criminally liable for non-compliance.

Are organisations in Singapore aware of their obligations under PDPA?

According to the 2017 Industry Survey on the Personal Data Protection Act (PDPA)[1] conducted by the Personal Data Privacy Council (PDPC) across 1,505 companies of various industry sectors and sizes in Singapore, while 92% of them are aware of their data privacy obligations, slightly more than half (51%) has appointed a Data Protection Officer (DPO). Most of them have some measures in place to handle personal data but only those with DPOs are more likely to comply across all nine obligations – Notify, Purpose Limitation, Consent, Accuracy, Access and Correction, Protection, Retention Limitation, Transfer Limitation and Openness.

In short, about half of organisations in Singapore are not able to comply to their obligations in accordance to PDPA and undergoing a **Data Privacy Impact Analysis (DPIA)** would have uncovered the gaps putting these organisations back on track to put in the people, process and technology in place to safeguard and protect personal data in their organisation.

Hidden Costs of Data Breaches Increase Expenses for Businesses

According to a global study in 2018 examining the full financial impact of a data breach on a company's bottom line conducted by IBM & Ponemon Institute, the hidden costs in data breaches – such as lost business, negative impact on reputation and employee time spent on recovery – are difficult and expensive to manage. The 2018 Cost of a Data Breach Study[2] found that the average cost of a data breach globally is $3.86 million, a 6.4 percent increase from the 2017 report.

What Impacts the Average Cost of a Data Breach?

For the past 13 years, the Ponemon Institute has examined the cost associated with data breaches of less than 100,000 records, finding that the costs have steadily risen over the course of the study. The average cost of a data breach was $3.86 million in the 2018 study, compared to $3.50 million in 2014 – representing nearly 10 percent net increase over the past 5 years of the study.

The study also examines factors which increase or

decrease the cost of the breach, finding that costs are heavily impacted by the amount of time spent containing a data breach, as well as investments in technologies that speed response time.

- The average time to identify a data breach in the study was 197 days, and the average time to contain a data breach once identified was 69 days.
- Companies who contained a breach in less than 30 days saved over $1 million compared to those that took more than 30 days ($3.09 million vs. $4.25 million average total)

The amount of lost or stolen records also impacts the cost of a breach, costing $148 per lost or stolen record on average. The study examined several factors which increase or decrease this cost:

- Having an incident response team was the top cost saving factor, reducing the cost by $14 per compromised record
- The use of an AI platform for cybersecurity reduced the cost by $8 per lost or stolen record
- Companies that indicated a "rush to notify" had a higher cost by $5 per lost or stolen record

The key take-away from the report is the cost of data breach is on the rise and with organisations frequently leveraging on multi-model channels from mobile to the internet to engage and interact with their customers, more personal data is collected across these channels and becoming more complex to manage and stay in compliance to data privacy laws.

It is therefore prudent for any organisation to examine it's data privacy policy, related processes, personnel and systems that falls into the nine obligations of PDPA and even engage an external organisation to assess and audit the whole systems and processes.

References:

[1] PDPC Industry Survey 2017

[2] IBM Data Breach Survey 2018 : https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

For further information or clarifications, kindly contact:

Gerald Tang Yew Hoong
Business Development Lead - Cybersecurity
BDO Advisory Pte Ltd
geraldtang@bdo.com.sg
+65 6828 9167

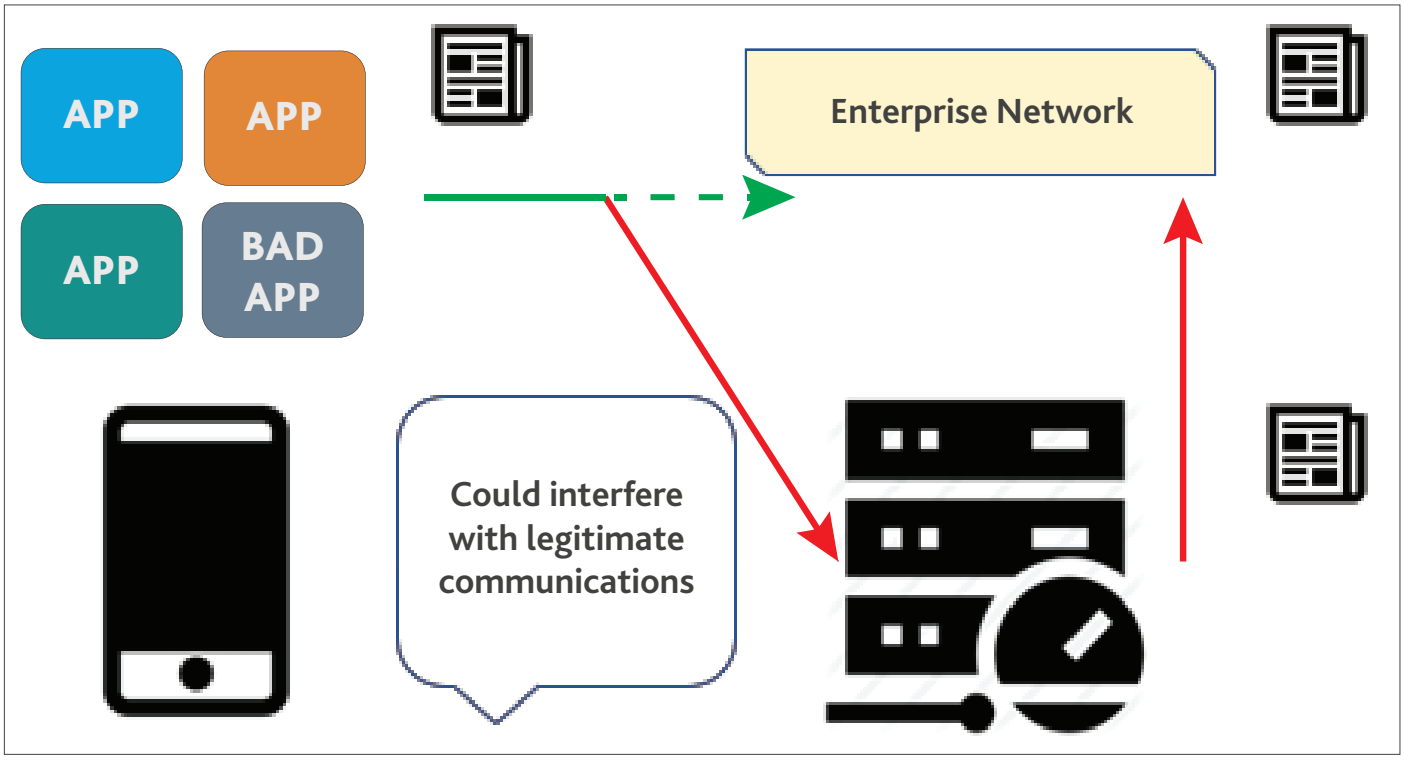
Protecting Your Data Security and Data Privacy

One of the most fundamental initial step in protecting your enterprise's data privacy and security is to first and fore-mostly identify the types of information you want to protect and where that information is exposed in your organisation. Once you have completed your review or audit - identified your organisation's priority information and determined your level of risk of data loss – then the next step is to assess your applications and understand what areas of your application portfolio are leaving you vulnerable to external attacks.

According to a recent Gartner report, the market for content-aware data loss prevention solutions continues to grow at more than 20 percent year over year. Yet the report also notes that many organisations are struggling to establish appropriate data protection policies and procedures for mobile devices as they interact with sensitive corporate data.

The threat model is different for mobile devices. There is much more risk of confidential data being stolen or leaked – where this is known as mobile data exfiltration. The additional risk is due to the portable nature of the devices, the types of applications and their usage models. Some of the significant differences between mobile devices and traditional computing environments include the following:

- Mobile devices are frequently shared temporarily. Even with PIN-protected devices, users can readily unblock their phones and hand them to other users.
- Mobile applications are highly connected to web services. This broadens the possible vectors for data exfiltration.



- Mobile devices are often consumer-owned devices that can access an organisation's internal network. Indeed, many enterprises are considering Bring Your Own Device (BYOD) programs as a cost-saving measure.

Due to these differences, traditional data protection and data security solutions are not readily applicable to mobile users. For example, the performance hit of an end-point agent on mobile devices would be unacceptable for most users. Similarly, forcing all mobile communications through the enterprise network for traffic analysis is not feasible. Datacenter-based solutions could identify confidential information resident on the device, but could do little to determine whether a personal application poses a genuine data loss threat to that confidential information.

Instead, what is needed is a solution that can assess mobile applications and determine if they represent a data loss risk to the organisation. For example, a mobile-based data protection and data security solution should identify applications that enable surreptitious transmission of microphone, GPS or camera data or data exfiltration via sockets, email, HTTP, SMS, DNS, ICMP or IR.

Effectiveness of Traditional Data Security and Data Privacy Products

The effectiveness of data security, data privacy and data protection hinges on:

- Accuracy of data loss prevention content analysis engines. Content analysis methods range from keyword searching, regular expressions handling and document fingerprint matching. Like any other analysis engine, lowering the false-positive and false-negative rates are important to improve the solution's accuracy.

- Scalability of data security solutions. As network traffic and employee use of multiple types of data grow, established data protection solutions must scale to keep up with organisational usage.

- Sophistication of the data security policy definition and process management capabilities. Organisations typically have multiple policies for different types of data and multiple processes to manage data and respond to data loss related events. The ability to automate policy enforcement in people- and process-centric situations is important.

Application Security and Your Data Security Strategy

Use this checklist as a reference tool when making data security buying decisions:

- Develop clear data security strategies with concrete requirements before evaluating products.
- Understand the limitations of traditional data privacy protection and data security. As an example, data loss prevention is a data-centric control and does not have any understanding of SQL.
- Applications protect your data. Test the security quality of your applications. Use application security testing as a way of protecting data.
- Create data protection policies and procedures for mobile devices as they interact with sensitive corporate data.

BDO Cybersecurity Helps Protect Your Data Security

The gateway to your data is through your applications. Attackers know applications are the weak link in today's IT networks and they look for vulnerabilities in applications that provide access to sensitive data. Testing applications for data security vulnerabilities reduce the risk of a data breach. Using BDO Cybersecurity as part of your data security strategy allows you to understand the data security quality of your applications and provides a path to improving the overall data security quality of all the applications running on your network and mobile devices.

For further information or clarifications, kindly contact:

Cecil Su
Director, Cybersecurity
BDO Advisory Pte Ltd
cecilsu@bdo.com.sg
+65 6829 9628

How CorpPass Affect Businesses?

With effect from 1 September 2018,all Government digital services can only be accessed via Singapore Corporate Access (CorpPass). CorpPass is a corporate digital identity for businesses and other entities such as non-profit organisations and associations to conduct online transactions with government agencies such as the Central Provident Fund (CPF), Inland Revenue Authority of Singapore (IRAS) and the Ministry of Manpower (MOM).

Why CorpPass?

Prior to this, there were 2 different sets of passes i.e. e-Services Authorisation System (EASY) and Singapore Personal Access (SingPass), in disparate systems to access Government to Businesses (G2B) digital services. As businesses have been using SingPass for corporate purposes, it creates a public concern whether it breaches the Personal Data Protection Act (PDPA) when sharing personal ID within a corporation.

Moreover, businesses require a common authentication and authorisation system to manage their user access for all G2B digital services. In light of this, the Singapore Government has launched CorpPass in September 2016.
What it meant to Businesses on IRAS myTax portal?
Businesses such as Singapore incorporated companies, Singapore branches, partnerships, etc. can now access myTax Portal to transact on the digital services with CorpPass, which they use to login using the EASY and SingPass. It is a good move in enhancing the security and individual privacy, in compliance with the PDPA, as well as to better protect and manage the corporate data. Apart from the Singapore entities, it allows the registration of CorpPass account for foreign entities so as to transact on myTax portal.

CorpPass has also introduced the CorpPass roles in an organisation i.e. Registered Owner (RO), CorpPass Administrator (Admin), CorpPass Sub-Administrator (Sub-admin) and Users, in managing

the CorpPass account. Employees/personnel of the businesses have to understand their roles and responsibilities in dealing with Government digital services.

Plus points

i. It is more secure as it allows Singapore-registered business owners to appoint employees to manage user accounts which are centrally managed and can be disabled instantly if compromised.

ii. It gives companies greater convenience, control and flexibility by providing a single platform to authorise and manage their employees' access to Government digital services.

iii. It enhances "cyber hygiene" with employees no longer using SingPass to transact on their company's behalf, leading to some sharing their SingPass details with one another.

Challenges

There are certain limitations when setting up or

transacting with CorpPass, such as:

i. Sub-admin with restricted access is unable to manage and assign the entity's digital services outside his/her assignment profile as well as authorising third party digital services. It is advisable if the functions of sub-admin can be improved to cater the business needs.

ii. More stabilised system - the system was unstable, especially due to high transaction volume. It could be enhanced so as to help the businesses in the transition process smoothly.

iii. Education/publicity - There are many businesses which have not registered for CorpPass account. More publications should be made to create the awareness among the businesses and workshops could be arranged to assist the businesses (especially Small and Medium Businesses) to transit onto CorpPass.

iv. Singapore entities without local contacts - It would be challenging in setting up a CorpPass account if there is no local contact with a Singapore entity, especially the CorpPass Admin must be a SingPass holder.

v. Registration of a CorpPass account for foreign entities - The registration is not operational as of September 2018. This would create additional pressure for foreign entities, especially since they need to meet the filing deadline for Goods and Services Tax returns and Corporate Income Tax returns in coming October and November 2018.

How can we help you?

As your business services provider, we act as the middleman between the businesses and the respective government agencies. We help to channel your feedback on the use of CorpPass for improvement.

Our Corporate Secretarial team may assist Singapore entities without local contacts in setting up and maintaining a CorpPass account. Do let us know if such need arises.

Moving forward

CorpPass has now gone live for all Singapore Government digital services!

It is indeed a good initiative to support Singapore's Smart Nation objectives and the Government's aim to create secured and reliable digital services for citizens and businesses as spelt out in the Digital Government Blueprint.

For further information or clarifications, kindly contact:

Evelyn Lim
Executive Director
BDO Tax Advisory Pte Ltd
evelynlim@bdo.com.sg
+65 6829 9629

Sin Chee Mei
Director
BOD Corporate Services Pte Ltd
cheemei@bdo.com.sg
+65 6828 9106

From OJEK to GO-JEK: Internationalisation may not be as far-fetched as you think

Article reproduced from ASME ENTREPRENEURS' DIGEST – Issue 81 (Sept/Oct 2018)

Home is where the heart is (and it's also opportunities are)

Economies are continuing to boom across Southeast Asia. According to the Asian Development Bank, Indonesia's economy is expected to grow 5.3% in both 2018 and 2019[1], due to improvements in investment and household consumption, higher export growth, a further decrease in unemployment levels and a lower inflation rate. Though the infamous traffic jam of Jakarta may spring to mind, the future is bright for this emerging economy, with President Joko Widodo pushing for a number of new road, air, sea and rail infrastructure projects to go ahead in the near future.

According to a recent ranking from the U.S. News and World Report, four of the top five Best Countries to Start a Business[2], globally, are in Southeast Asia:

Ranking	Country	GDP, USD	Population	GDP Per Capita, PPP, USD
1	Thailand	$406.8 billion	68.9 million	$16,885
2	Malaysia	$296.4 billion	31.2 million	$27,292
3	Mexico	$1.0 trillion	127.5 million	$18,935
4	Indonesia	$932.3 billion	261.1 million	$11,717
5	Singapore	$297.0 billion	5.6 million	$87,832

Malaysia and Thailand have projected GDP Growth Rates of 5.0 and 4.1%[1] respectively. Malaysia, too, is ambitious with its infrastructure development plans: developing the second phase of its Mass Rapid Transit line as well as planning to embark on a third phase simultaneously. While the country's economy has seen unprecedented growth, its property market continues to face challenges with the Association of Valuers, Property Managers, Estate Agents and Property Consultants in the Private Sector Malaysia, estimating that unsold property is now worth approximately RM35.5 billion[3] .

By and large, thanks to tourism. Thailand's hotel and

restaurant sector is expanding at an accelerated rate, growing by 13.5%[4] during the course of 2017.

So why aren't we making the most of it?

Knowing what our region has to offer, it is interesting to note that only 14% of local SMEs intend to internationalise, according to QBE Insurance's recent survey of Singapore's SME business leaders[5].

Internationalisation is within reach if you know which foundations to lay

The key foundations of internationalisation are as follow:

1. **Know your company**

   It is important to understand your motivations behind internationalisation. Reasons such as 'everyone else is doing it, so I should too', or 'my product is successful in Singapore, therefore it will succeed anywhere' do not necessitate the foundations of a successful internationalisation strategy. Rather than reacting to the current market, it is worthwhile taking measured steps to ascertain what would add the most value to your growing business. Do you have a successful business model in at least one existing market, and do you have the time and resources (both capital and manpower) to invest in a new market for up to three years to ensure success?

2. **Get to know your customers**

   Misunderstanding cultural differences such as demographic split, language preferences and religion could make or break your business. Understanding customer preferences and pricing sensitivity as well as the local distribution channels available, will be invaluable for tailoring your products to the local market. To overcome this barrier, in fact, many companies choose to work with a local partner to gain maximum expertise and penetration in new markets.

3. **Map out your competition**

   You may already know who your key competitors are, but are you confident in your competitive edge going into this new market? Finally, is your intended market on a steady growth trajectory? Do you know if economies of scale are accessible?

From ojek to GO-JEK

GO-JEK has recently vowed to invest US$500 million into its international expansion strategy, to include Philippines, Singapore, Thailand and Vietnam[7]. Contrary to Uber and Grab; their internationalisation strategy will be to select partners on the ground to found their operations, while GO-JEK will act more as an advisor by contributing its technical support and expertise to the partnership. As it is likely that its success in Indonesia was born out of the unique traffic situation of the country, GO-JEK will need to rely on the deep and unrivalled knowledge of these local partners to ensure its products continue to remain relevant.

Starting in 2010 with just 20 ojek drivers, GO-JEK has not raised more than US$2 billion to date. Due to extensive market research, GO-JEK identified that the consumers in these four Southeast Asia countries were not satisfied with the current ride-hailing options

available to them. Rather than rushing to expand across the region like some of its counterparts, GO-JEK took time to know itself and establish a successful business model. Hence it has successfully cemented itself as a ride-hailing and multi-services platform market leader. GO-JEK was clearly willing and able to know its customers by adapting to the local market, and there was sufficient funding to be in it for the long run. As for mapping out its competition, we will have to wait and see just how much market share Grab is willing to give up.

It doesn't matter whether your SME is a start-up or an established multimillion-dollar company. As long you you lay your foundations, internationalisation should no longer be a daunting prospect as you are already more than halfway there.

References:

1 Asian Development Bank (ADB)'s flagship annual economic publication, Asian Development Outlook (AD) 2018
2 https://www.usnews.com/news/best-countries/start-a-business-full-list
3 https://www.straitstimes.com/asia/south-east-asias-roaring-economies
4 NESDB ECONOMIC REPORT, Thai Economic Performance in Q4 and 2017 and Outlook for 2018
5 http://www.qbe.com.sg/retrieveDocument?docName=SME_press_release_and infographics_29_Jan_2018.pdf
6 http://aseanlegalalliance.net/invest-in-south-east-asia/
7 https://ww.GO-JEK.com/blog/expansion-into-four-new-markets/

For further information or clarifications, kindly contact:

Claire Scott
Assistant Manager
BDO Consultants Pte Ltd
clairescott@bdo.com.sg
+65 6828 9118 extn 838

CONTACT US

BDO LLP
600 North Bridge Road
#23-01 Parkview Square
Singapore 188778
Tel: +65 6828 9118
Fax: +65 6828 9111
info@bdo.com.sg

www.bdo.com.sg

CONNECT WITH US.

Like us, follow us, engage us through our social media channels: