



BDO CONNECT

#DeadMenDataPrivacy - Data of the dead still matters and requires data protection (from the living)?
Page 2 to 4

Compliance Requirements of Frequent Business Travellers
Page 5 to 7

Changes in Employment Act with effect from 1 April 2019
Page 8 to 9

MANAGING PARTNER'S MESSAGE



Frankie Chia
BDO Singapore

In February, we had the Budget 2019 which was announced by the Finance Minister. The immediate reaction from the business community and analysts alike is that it was a continuation of the government effort towards restructuring, transforming and strengthening the society and the economy. Although low on significant tax changes it has various targeted measures aimed at helping Singaporeans manage healthcare costs and other expenses, as well as supporting businesses and workers, succeed in a rapidly changing business environment. SMEs remains focus in this Budget with programmes such as the Innovation Agents Programme, SME Co-Investment Fund, SME Go Digital Programme; geared to help companies tap on emerging opportunities and position Singapore as a "Global-Asia node of technology, innovation and enterprise". I hope you have taken advantage of our budget analysis published on our Budget Bulletin and Commentary released for you just after the Budget. As usual, if you need help on the recently announced tax changes, our tax professionals are ready to help.

From time to time, we hear incidences of data breaches incidences in the news. And of late the health records seem to be in focus. Thus, in this issue, we decided to include an interesting article which tends to overlook. I am referring to the data belonging to those that have passed on. I invite you to read it and understand how cybercriminals find those data extremely useful for their criminal objectives. Read on!

CONTENTS

#DeadMenDataPrivacy - Data of the dead still matters and requires data protection (from the living)?

Compliance Requirements of Frequent Business Travellers

Changes in Employment Act with effect from 1 April 2019

The Advantages and Disadvantages of Family Business

#DeadMenDataPrivacy - Data of the dead still matters and requires data protection (from the living)?



As the saying goes “Dead men tell no tales” put forth the notion a dead person cannot reveal secret information. While it is true a dead man’s password follows him to his grave, his personal data might live on for a longer period than we think. Why are we taking notice of the dead all of a sudden? Is this an article not looking at cybersecurity impacting the living and enterprises serving the living? Are we getting morbid and obsessed with the dead?

Let’s take a step back and review the information engraved on the tombstones and the niches, you have the name of deceased, date of passing, and for

some, the place of birth (province and state). What good is this information and who might be interested in details of the dead to exploit for malicious intent?

It is no surprise personal identifiable information is a big commodity on the Dark Web, even for the deceased. Medical records are now becoming even more popular than credit information. The stolen medical records – of the living — for sale on black markets remain a huge problem. The three local data leak incidents from the healthcare sector in recent news here comes to mind. We can all understand why the health information of someone living could

be valuable. But what is to be gained from the information about someone already dead?

Security vendor Cynerio¹ found a post from a vendor on the dark web offering 60,000 medical records of the deceased, including their death dates. The reason why is when it comes to identity theft or running up fraudulent charges there is no better victim than one that can't file a complaint. Fraud like this can go unnoticed for a very long time. With this type of information, fraudsters can attempt open credit card accounts, apply for loans, commit tax fraud and obtain expensive mobile phones via carrier contracts. In addition to financial fraud, stolen medical records fraudster can use for acquiring medical supplies and securing health insurance illegally. Criminals on the dark web have been found explaining to potential customers in some countries how they can use a medical ID to get prescribed drugs delivered to them, to order medication and even to book a doctor's appointment for a check-up.

With the proliferation of social media and ancestor worship going online, we have seen many web portals being in China set up to facilitate commemoration and paying respects to the deceased. For example in China, one of the popular portal created allow friends and relatives to commemorate the dead through leaving a message, virtual bouquet and wreath, and virtual items that helped to remember the deceased. These web portals hold a treasure trove of information about the dead and the eulogies being written further allow to uncover accurate profile like what one can find from a Facebook profile.

All of this shows that it is crucial for healthcare organisations and service providers to be aware of this growing demand for Personal Identifiable Information (PII) of the living, as well as the deceased, to beef up their cybersecurity strategies.

Taking a more preventive approach, BDO would suggest all organisations, in particular, those in healthcare, to take a holistic view of data protection in their cybersecurity strategy. Some recommendations, not an exhaustive list but key takeaways, would be to look at:

- **Security hygiene.**

As seen in some of the recent data breach incidents in the healthcare sector, common hygiene issues can undermine advanced security capabilities.

For a start, an enterprise should always download software from trusted sources and avoid using unfamiliar free or pirated software. Keep all systems and devices up-to-date by rapidly applying the latest updates to the operating systems (OS) and applications, and immediately deploy critical security updates for OS, browsers, and email. More importantly, isolate (or retire) devices that cannot be updated or patched and deny access to the corporate network.

Enterprises should implement advanced email and browser protections too. Deploy a secure email gateway that has advanced threat protection capabilities for defending against modern phishing variants. Ransomware, most prevalent malicious software used by hackers to lock up a computer, in particular, gets dropped into an organisation through malicious email sent from emails with familiar but spoofed domains. Enable host anti-malware and network defences to get near real-time blocking responses from the cloud.

- **Be vigilant and raise overall cybersecurity awareness.**

A long-term phishing study in the United States involving six healthcare institutions shows employees are vulnerable to phishing attacks,

¹Source : Healthcare Hacking Trends on the Dark Web (<https://cynerio.co/healthcare-hacking-trends-dark-web/>)

and that they can become more vigilant through exposure. Enterprises certainly do not need to become a victim of a cyber attack to become more vigilant. By conducting periodic cybersecurity awareness training and teaching employees to be wary of suspicious communications that request sensitive information and instruct them on how to respond and report them to the organisation's Security/ IT team immediately. Moreover, such periodic training can help mitigate social engineering and spear phishing attacks. Teach employees to practice secure web browsing habits using solutions that provide warnings about or block access to unsafe sites can help reduce the probability of encountering websites associated with cryptocurrency mining. If an employee observed that his/her computer is running exceptionally slow, alert Security/ IT team to look for any suspicious files that are running and call in outside help if needed.

- **Keep backups.**

Create destruction-resistant backups of your critical systems and data. Use cloud storage services for an automatic backup of data online. For data that is on premises, regularly back up important data using the 3-2-1 rule - Keep three backups of your data, on two different storage types, and at least one backup at an offsite location.

Most, if not all, of the data breaches, happen because of either "System Foul-ups" or "Human Slip-ups". The former can be addressed with better Security Hygiene and the latter better handled with educating employees to be more vigilant and raise overall cyber security awareness in the organisation. Lastly, the least any organisation can help itself is have a fallback option that can potentially save its business operations in any cybersecurity attack – BACKUP data.

For further information or clarifications, kindly contact:

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

Compliance Requirements of Frequent Business Travellers



Background

Businesses and companies now operate in an increasingly global environment where employees work across borders with greater ease. Consequently, ensuring compliance with destination countries' regulations (e.g. immigration, social security, taxes, etc.) is more important than ever.

Over the years, Singapore's various government agencies, including the Inland Revenue Authority of Singapore ("IRAS"), have reviewed and revised the requirements and employer's obligations in respect of frequent business travellers ("FBT"). A FBT is defined as an employee who is based outside of Singapore and makes frequent business trips into Singapore. Although Singapore does not have monthly withholding requirements, companies still face risk in the other areas relating to FBTs travelling to Singapore for business purposes.

Immigration

An employment pass ("EP") has to be obtained before an individual can carry out work in Singapore regardless of the duration of the stay. The only exception to this is where the intended work is the following:-

- Company meetings, corporate retreats or meetings with business partners;
- Study tours or visits as a participant;
- Company training courses/workshops/team building events as a participant;
- Seminars and conferences as a participant;
- Exhibitions as a trade visitor.

Aside from the above, an EP has to be obtained before the FBT's arrival into Singapore. Generally, an FBT cannot carry out any employment activities in Singapore without an EP.

Tax Reporting And Filing Obligations

An annual review of all FBT's business days into Singapore is to be done by 31 January of the following year by the employer. The individuals would, therefore, fall into the following categories depending on their number of business days:-

Individuals with not more than 60 business days in a calendar year in Singapore

Under section 13(6) of the Singapore Income Tax Act, employment income is exempt from Singapore tax if the individual is a non-resident for tax purposes and does not exercise employment for more than 60 days in a calendar year. This does not apply to a non-tax resident director or public entertainer.

If the employee does not hold an EP, as an administrative concession, there is no employer's reporting requirement to the IRAS. An employing entity has to submit to the IRAS for all FBTs with valid EP as at 31 January of the following year, the details including their respective travel dates into Singapore. An employer has to submit all these details by 1 March of the following year. Additionally, upon cancellation or expiry of the EP, the employing entity is to notify the IRAS within two months of the cancellation/expiration to prevent any enforcement actions by the IRAS.

Individuals with more than 60 days but less than 183 days in Singapore

Where an individual has more than 60 business days in Singapore but less than 183 days, he is liable to tax on his employment income earned in respect of his business days in Singapore. He will be taxed on this income at the non-resident tax rate. A tax exemption could be possible to the extent that the employee qualifies the criteria under the relevant Avoidance of Double Taxation Agreement ("DTA") that Singapore has with a relevant country. This

is typically the country where the individual is tax resident in, and where his employment is based. Where a treaty exemption is available, the employer must make an application on employee's behalf to the IRAS before the filing deadline on 15 April. All employees with such number of travel will very likely be engaging in activities that require an EP.

In respect of the filing requirement, the filing of the FBT's Return of Employee's Remuneration (Form IR8A) is required by 1 March together with the rest of the regular employee population unless a Form IR21 is applicable in an EP cancellation or expiry case. As part of the tax clearance process, a Form IR21 (Notification of a foreign employee's cessation) should have been filed at least two months from the date of cancellation or expiry of EP; and this has to be done immediately if not already done unless a request for an extension is obtained.

Once it is certain that a FBT would no longer make business trips into Singapore, his employer should cancel his EP, and a Form IR21 filed within two months from his final business day in Singapore.

Individuals with more than 183 days in Singapore

These are FBTs, who have more than 183 business days in the preceding calendar year and still have a valid EP at the time of the employer filing the employees' Form IR8E. The filing requirement and deadline for this group will be the same as all regular employees. This group of employees will not be able to avail to the exemption under the Double Tax Treaty; his employment income will be taxed at the resident rate.

Under Section 2(1) of the Singapore Income Tax Act, an individual is regarded to be a tax resident in Singapore in the year he is physically present or exercising employment in Singapore for at least 183 days in the preceding calendar year.

Taxable Income

From 1 January 2016 onwards, the IRAS has revised the tax treatment of compensation provided to a FBT. Currently, the following items are not taxable to the FBT:-

- Airfare
- Accommodation
- Transport and entertainment allowance for business purposes
- Per diem within the acceptable rate laid out by the IRAS (the excess per diem is taxable)
- Other reimbursements for business expenses

Aside from the above, any other compensation provided to the FBT is taxable in Singapore and required to be reported to the IRAS unless the FBT qualifies for tax exemption.

Social Security (Central Provident Fund)

The Central Provident Fund ("CPF") is a mandatory savings scheme for working Singapore citizens and Singapore permanent residents in Singapore. All foreign individuals are not allowed to participate in this scheme. However, upon becoming a permanent resident of Singapore, participation in the CPF would be compulsory.

In addition, should a Singapore citizen or Singapore permanent resident who is based and working for an overseas employer make business trips into Singapore, CPF contributions is not required to be made by the employing entity. However, both employer and FBT employee can continue with voluntary contributions into the CPF.

BDO Comment: Next Steps

Due to difficulties in tracking these FBTs and a lack of understanding and knowledge of the reporting requirements for FBTs, the risk of non-compliance is high. Such risk may lead to a loss of the company's reputation and heavy penalties and even prosecution; in some cases, this can cause business disruption. Companies should review the current process to manage these FBTs and to ensure immigration and tax/social security compliance.

Some preliminary questions which the company can ask:-

1. How are the business days of travellers being tracked?
2. Is the appropriate work pass being applied for being a FBT travels?
3. What are the compensation items provided to FBT during the trips?
4. Is the company familiar with the various compliance regulations?
5. Is there any possible corporate tax implications (i.e. Permanent establishment) in the destinations of the FBT?

For further information or clarifications, kindly contact:

Wu Soo Mee
Executive Director
People Tax Advisory
soomee@bdo.com.sg
+65 6828 9125

Changes in Employment Act

with effect from 1 April 2019

How the Employment Act (EA) changes in 2019 will affect you:

(I) Extension of Core Provisions of the EA to Protect All Employees

BEFORE	AFTER
Employment Act does not cover managers and executives (M&Es) earning above \$4,500 a month	The \$4,500 per month salary cap on managers and executives (M&Es) will be removed

(II) Extension of Part IV of the EA to Protect More Employees

Enhance the protection of working hours, payment for overtime work and rest days for non-workmen:

BEFORE	AFTER
Applicable to workmen earning a basic salary up to \$4,500/month	No change
Non-workmen earning a basic salary up to \$2,500 a month and overtime rate payable capped at \$2,250 a month	Non-workmen earning up to \$2,600 a month and overtime rate payable capped at \$2,600 a month

(III) Enhancement of the Employment Dispute Resolution Framework

BEFORE	AFTER
Wrongful dismissal claims are heard by the MOM, whereas salary-related claims are heard at Tripartite Alliance for Dispute Management/ Employment Claims Tribunals (ECT)	Wrongful dismissal claims and salary-related claims will be heard at the Tripartite Alliance for Dispute Management/ Employment Claims Tribunals (ECT)
M&Es can seek help if they have served the employers for at least a year	M&Es can seek help if they have served the employer for at least six months

(IV) Adopt Less Prescriptive Approach for Authorised Deductions

BEFORE	AFTER
Employers can make salary deductions only for specific reasons under the EA.	Employers can also make salary deductions if they: <ul style="list-style-type: none"> a) Obtain written consent from their employees; and b) Enable employees to withdraw their consent anytime, without penalty

(V) Enhanced Flexibility for Employers

Extend option of time off for working on public holiday to more employees

BEFORE	AFTER
For work on public holidays, employers can offer time-off only to M&E's earning up to \$4,500 a month.	For work on public holidays, employers can offer time-off salary to:- <ul style="list-style-type: none"> - All M&Es - Workmen earning above \$4,500 a month - Non-workmen earning above \$2,600 a month

(VI) Other Amendments to the Employment Act

BEFORE	AFTER
Employer only recognise medical certificates issued by: <ul style="list-style-type: none"> - government doctors and - company-approved doctors 	Employer must recognise medical certificates issued by: <ul style="list-style-type: none"> - any registered doctor and dentist Clarifying that paid hospitalisation leave is to cover: <ul style="list-style-type: none"> - The period requiring hospital care and the period of recuperation after being discharged; - Quarantine orders as required by law; and - Situations where the hospital doctor assesses that the patient is ill enough to require hospitalisation but is not hospitalised

For further information or clarifications, kindly contact:

Lim Mei Khim
 Director
 Business Services Outsourcing
 meikhim@bdo.com.sg
 +65 6828 9109

The Advantages and Disadvantages of Family Business

There are many successful family business cases out there in Asia, large organisations such as Hyundai Group, Samsung, Wahaha Group, Hong Leong Group as well as LKK Group which is known for its Lee Kum Kee sauces are some examples of companies listed on stock markets in the region and have surpassed their competitors in the market. Looking at how successful these businesses can be, there are proven successes of family businesses that make it lucrative for one to be in. Are there more benefits to working in family businesses than this?

Collaboration and Compromise

Blood relatives, or marriage partners – these are the people whom you will face on a daily basis at home, and at work if you work in a family business. Since you know family members well enough, this cuts down the need for employee orientation, or a warm-up time needed for new-joined employees, who are your family members. Knowing and being aware of each family member's characteristics, strengths and weaknesses make work discussions easier, makes allocation of tasks more accurate and also the sharing of information more comfortable and free.

Strong common incentives

Being a member in a family business, also means all members are well-aligned, and carry the same aspirations for the business – to contribute to a firm that is able to ensure success of the family and even several generations later. In order to ensure that the firm remains 'available' for the family for multiple generations to come, family business management tend to have longer visions and plans for the business. Family members who are also the major shareholders of the firm will work for the common incentives as they are the main benefactors should their business flourish.

Strong commitment and higher rewards

In order to sustain the forefather's heritage and business, family members are often committed and loyal to ensure the success of the organisation. Many family members' work round the clock and their tenure in the firm are usually substantially longer as compared to employees in multinational companies, in which the turnover rate for directors and managers are high. Other than that, to reward for hard work, the compensation package family



members receive are usually higher as compared to market rates. On a longer term point of view, family members also hold their positions for years and those who have garnered sufficient years of experience with the business have built strong relationships and networks with stakeholders, customers and the other firms in the industry.

These are some examples of working in family businesses. It may seem to have numerous advantages, nonetheless, there are many downsides to it as well.

A pivotal challenge that many family businesses face is successful succession planning.

There is a Chinese saying that 'wealth never survives three generations'. Succession in family businesses does not only refer to a transfer of leadership, but a transfer of ownership from one generation to the next. As the business gets handed down to generations down the years, together with the change in leadership and stakeholders, the interests and goals of the business changes.

Along with the handover of the family business, elders may be resistant to changes proposed and decisions made by the successors and start to question the successors' capabilities and also compare with their personal work process. Such resistance may hinder the transition process of leadership between generations and impact the business.

Another challenge that family businesses go through is conflict management.

The different views in business growth, needs, expectations, mixed with personal views such as values, and different upbringing in family members often lead to conflicts and tension among each other. For example, siblings in the same household

may be brought up and hence share the same family values. However, cousins may differ as they live in different households whose families have differences in values, views and upbringing. Often times, differing views result in conflicts especially if the parties are not willing to compromise with each other. Other than that, gaps in communication and failures to manage each other's expectations arise to conflicts.

Such conflicts and tensions will not only emotionally impact an individual but also sours family and business relationships, which eventually harms the family business.

Although many family businesses have dominated various industries and performed outstandingly in the stock markets, we all understand that succession between generations is always a crucial phase for many, if not all family businesses. It is unsurprising that many family businesses failed at this phase to make it into the next generation. Through the phases, it is crucial for all parties to be open to different opinions, values, needs and expectations and compromise with each other to successfully transit along with the changes that occurs during succession.

*For further information or clarifications,
kindly contact:*

Low Hui Xin
Consultant
BDO Consultants Pte Ltd
huixin@bdo.com.sg
+65 6828 9118 extn 801

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

Disclaimer: This newsletter has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO to discuss these matters in the context of your particular circumstances. BDO, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone reliance on the information in this publication or for any decision based on it.

Copyright © 2019 BDO LLP

BDO LLP (UEN: T10LL0001F) is an accounting Limited Liability Partnership registered in Singapore under Limited Liability Partnership Act (Chapter 163A). BDO LLP is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

CONNECT WITH US.

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

