Reasons Behind Poor Cybersecurity Readiness of Singapore's Small Organizations: Reveal by Case Studies

Nam-Chie Sia[1] Amin Hosseinian Far[2][0000-0002-2534-9044] and Teoh Teik Toe[3]

[1,2] University of Northampton, Northampton NN1 5PH, UK
[3] Amity Singapore, 101 Penang Rd, Singapore 238466
[1]sia_nam_chie@hotmail.com, [2]Amin.Hosseinian-Far@Northampton.ac.uk, [3]Teohteiktoe@gmail.com

Abstract: Digitalization and cybersecurity are two important trends that are affecting the business world tremendously. Digitalization, which drives data analytics, provides opportunities for organizations to create new models to beat competition. On the other hand, cybersecurity is a threat to organizations' financials, operations, and reputation. COVID-19 has accelerated the adoption of digitalization, which has opened up more opportunities to hackers for cyberattacks. In another word, digitalization underlines the importance of cybersecurity. With the foresight of the government, Singapore has promoted cybersecurity as one of the pillars for the nation's total defence to signal the government's attention and resources committed to fight against cyberattacks. Notwithstanding the effort from the government, losses due to cyberattacks continue to rise. Furthermore, the network of the biggest healthcare provider in the country was compromised and its data, including that of the Prime Minister, was stolen. For small organizations where resources may be limited, the risks are even higher, pointing to the urgent need to address the situations. Therefore, this article uses two small organizations in Singapore as case study, to draw insights on the obstacles to implement digitalization and cybersecurity. With the insights, actions that can be taken by government, businesses, and academies, are proposed to improve the digitalization and cybersecurity of small organizations, in Singapore and elsewhere.

Keywords: Cybersecurity, Data analytics, Digitalization, Small Organization, Singapore

1 Introduction: Digitalization and cybersecurity trends

1.1 Global

It is well-known that the current world is being disrupted by new business models driven by digitalization. As organizations digitalized, more activities are being captured electronically (LaValle et al, 2011), which enable the organizations to use insights drawn from data analytics to provide better services and products to customers, thus outperform their competitors (Lemieux et al, 2014).

The COVID-19 pandemics has accelerated the adoption of digitalization (IBM 2020; Lambert, 2020). Therefore, it is foreseeable that more consumers' activities will be captured digitally for data analytics, supported by machine learning and artificial intelligence capability, to assist companies to gain competitive advantages.

Some of the popular examples are companies such as Amazon, Airbnb, Nexflix and Uber, who use data analytics to alter the competitive landscape (Gartner, 2018) create competitive advantages over their competitors (Hair, 2018).

With digitalization and data analytics, the world has become more connected. However, on the flip side, the risks and costs of cyber threats, where hackers can steal data from anywhere in the world, have increased tremendously. The risks are compounded as many organizations are adopting the "work from home" protocols due to COVID-19 pandemics (CSA2, 2020).

1.2 Singapore

Singapore is a small country, located in South-east Asia, who was granted self-governance by the United Kingdom in 1959, and gained full independence in 1965. Although it has little natural resources, the country progresses economically and socially, due largely to the government's leadership. The gross domestic products (GDP) per capita grew from US$400 in 1959 to US$22,000 in 1999 (Lee, 2000), and to US$64,000 in 2018 (DOS, 2018).

Singapore has a pro-business government, who is able to execute policies in a consistent manner to garner confidence from multi-national companies (Lee, 2000). Sensing that digitalization and the power of data analytics are going to impact businesses, the government has launched a "smart nation" initiative to drive the entire nation to embrace digital transformation, as the government believes this will improve the lives of its population, create more jobs and enhance engagement with communities (Lee, 2014).

Singapore has not been spared from cyberattacks. In 2017, Singaporeans have fallen victims to various schemes, such as phishing, malicious software, and ransomware, which caused losses amounting to approximately US $30 million (CSA, 2018). Between May and July 2018, personal data of approximately 1.5 million patients of SingHealth Group, the largest healthcare service provider in the country, was illegally accessed and copied (ST, 2018). Among the patients whose data was breached, was the country's prime minister, who was specifically and repeatedly targeted (CSA2, 2020).

In response to the cybersecurity risks, the government has promoted digital defence as the sixth pillar to the nation's Total Defence Framework (CSA1, 2020). Specifically, the government has led initiatives to formulate Operational Technology Cybersecurity Masterplan 2019 to build a resilient infrastructure, and raise awareness to create a safer cybersecurity environment.

1.3 Small organizations in Singapore

With regards to digitalization and data analytics, despite the "smart nation" initiative launched by the government, studies have shown that a substantial proportion of organizations, especially the small and medium-sized enterprises (SMEs), have not adopted digitalization and data analytics (Ramchandani, 2017). It was found that 43% of the Singapore SMEs are not familiar with the term "digital transformation" (Microsoft and ASME, 2018) and 85% of Singapore workers are not confident to perform data analytics (Shivkumar, 2019). Microsoft and ASME (2018) further revealed that key decision-makers in small enterprises have much lower awareness of digitalization than their counterparts in medium-sized organizations. In fact, other than staff who work in the information technology department, the majority of the staff in small organizations find it challenging to understand digital transformation (IBM, 2020).

As Singapore prides herself as the gateway to South-east Asia and being one of the world most digitally connected cities (CSA3, 2020), the low awareness of digital transformation and data analytics are worrying, as it shows that a pocket of the nation has not been keeping up with the rest. The situations are even more dire in term of cybersecurity, as pointed out by the Cyber Security Authority (CSA) of Singapore, the majority of the cyberattack victims in Singapore are SMEs (CSA2, 2020).

2 Rationale, aim, objectives and methodology of study

2.1 Rationale

As small organizations in Singapore have comparatively low adoption rate of digitalization, it is worrying trends that the small organizations account for the majority of cyberattack victims. There is an urgent need to help these small organizations to gain competitive advantages in the digital world in a safe and secured manner. This is because SMEs employed two-third of the nation's workforce (Teo, 2013) and contributed to approximately half of her GDP (Microsoft and ASME, 2018).

Being the collective employers for two-thirds of the workforce, SMEs cannot be left behind in the digit transformation era. They also cannot continue to be the main victims of cyberattacks.

In addition, although studies on cybersecurity for SMEs are not new, our literature review shows that there is little being done in the Singapore context.

2.2 Aim

This study aims to identify and understand the root-causes of the low adoption rate for digitalization, and yet being the main victim of cyberattacks. Understanding the causes of the problems can help to formulate effective solutions to address the issues, as the first step of a change journey is to understand the situations and identify the problems (Moore, 2011).

While this study is performed in Singapore, it is believed that the lessons learnt can be references for small organizations in other countries.

2.3 Objectives

With the aim to identify and understand the root-causes, the objectives of this study include:

- Identify the root-causes of low adoption rate of digitalization and cybersecurity for small organizations in Singapore
- Inquire board members and senior management of small organizations to understand the challenges from their perspective

- Propose practical solutions to raise adoption rate of digitalization and cybersecurity in small organizations

2.4 Methodology

There is little study on the adoption of digitalization and cybersecurity for small organizations in Singapore, hence, this exploratory study will adopt qualitative methodology using case study method.

Qualitative research methodology is suitable for explorative and descriptive research (Al Zefeiti and Mohamad, 2015). It is also the recommended methodology to develop understanding, especially when there is little prior knowledge or research (Basias, 2018; Kerr et al., 2010).

Case study method is also appropriate for exploratory, explanatory and descriptive researches (Tellis, 1997; Yin, 2003). In addition, case study is recommended for research that is focusing on real-life issues (Yin, 1984), especially when limited knowledge exists (Marrelli, 2007), and when in-depth investigations are required (Dasgupta, 2015). In addition, learning can be achieved through practical reflection (Raelin, 2015) and practitioners are encouraged to use reflection-in-action to discover new knowledge (Castley et al, 2010).

The case study for this paper uses two small organizations in Singapore, with different financial resources and organization culture, to compare and contrast their readiness to adopt digitalization and cybersecurity.

The main data collection techniques are interview and archival record. Interview is adopted because it is more aligned to qualitative research, which tends to be exploratory (Azorin, 2007), and it is the most important data collection methods in case study (Tellis, 1997). However, other data collection techniques should be used to supplement those collected via interviews (Oplatka and Hemsley-Brown, 2004). Therefore, the authors also collect evidences using archival records to authenticate and corroborate those obtained from interviews.

After understanding the challenges, this study proposes actions that could be taken to raise digitalization adoption rate, and the cybersecurity standards of small organizations in Singapore.

3 Literature review

3.1 Digital transformation in Singapore

As the world in embracing digitalization, the Singapore ministers have been encouraging its communities, including SMEs, to embark on their journey in digital transformation and data analytics (Lung, 2018), to gain competitive advantages (Tan, 2016) and as a result, be a new engine for growth in Singapore (Ong-Webb, 2017).

Despite the encouragement, and support provided, by the government to embrace digitalization, the paces of adopting digitalization and data analytics among the Singapore SMEs are slow (Microsoft and ASME, 2018; Ramchandani, 2017;

Shivkumar, 2019). This trend is alarming, as the Singapore SMEs are running the risk of being left behind and losing out to their competitors (DBS, 2018; OECD, 2017). This is on the back that digitalized organizations are more productive than those who do not, as well as customers' increasing expectations for more personalized services that can only be provided through insights from data analytics (Alibaba Cloud, 2018). Therefore, SMEs who are not embarking on digitalization may not survive the competition in the near future.

Some of the factors attributable to the slow take up rate include lack of financial resources, constrain in staff resources, and availability of committed sponsors (Sia, 2018)

3.2 Cybersecurity

As organizations are embracing digitalization and data analytics to gain competitive advantages, this transformation has permeated to almost every industry. Along the growing trend where business organizations embrace digitalization, cybersecurity becomes a significant business issue that impacts customers, profitability, and reputation (Lanz, 2014). Cybersecurity can include many aspects such as data protection, integrity, confidentiality, encryption and fundamental security functions (Bhattacharjya et. al., 2019)

Cybersecurity affects all industries and organizations of all sizes, including small business (Al-Moshaigeh et. al., 2019). This assertion is similar to the evidence shown in Singapore, where the small organizations accounted for the majority of cyberattack victims (CSA2, 2020). The threats of cybersecurity, which include disruptions to businesses, negative publicity, litigation, and long-lasting reputational damages (Lanz, 2014), can be costly for small organizations as they have little resources at their disposal (Al-Moshaigeh, 2019). It is a vicious cycle that due to the limited resources to strengthen their cybersecurity, small organizations are increasingly being targeted (Bada and Nurse, 2019).

There is indication of the poor cybersecurity readiness in the small organization can be attributable to the poor awareness because they are too immersed in their day-to-day operations and did not spend enough time to proactively study emerging risks (Bada and Nurse, 2019). The lack of awareness then leads to delay the investment in security and give priority to other urgent tasks (Lanz, 2014).
Common types of cyberattacks

Phishing

Phishing is the most common type of attack. It is a form of social engineering where the hackers pose as a trustworthy organization (Lanz 2014). For example, phishing can be initiated via an email that appear to be coming from a bank or government agencies to trick the victims to click on dubious links or attachments (CSA, 2018). Once the victims clicked on the links or opened the attachments, a "secret" program will move into the laptops or devices without alerting the victims. From there, the hackers can control or steal data from the victims' laptops or devices. Alternatively, the hackers can persuade the victims to disclose their confidential information, which will be used to access the victims' bank accounts or other information stored online.

A common consequence suffered by victims of phishing is to surrender the control rights of their organizations' websites to the hackers, who show little hesitance to alter or deface the websites. Unauthorized access and intentional alteration of information without rights are considered cybercrime (Jahankhani et. al. 2014). For individuals, after disclosing their confidential information such as their bank account passwords to the hackers, they may lose their hard-earned money in their bank accounts.

In 2019, CSA detected an increase of 200% of phishing over the number in 2018 (CSA2, 2020). The situations just got worse. In the first half of 2020, the number of cyber scams has increased by 2,500% compared to the same period one year ago (CNA, 2020).

Malicious software

Malicious software, or commonly known as malware, are programs that allow the hackers to control the laptops or devices, by compromising the security of laptops or devices, without the victims' knowledge (CSA, 2018). It was noted that some of the malware were first detected 10 years earlier continue to successful attack the victims in 2017, indicating that the victims did not the updated their scanning software to clean up their systems (CSA, 2017).

The malware can also deny the access by the genuine owners of the devices. They do so by using algorithm to encrypt files that deny the owners' access unless they know the passwords (CSA2, 2020). The hackers normally demand a certain amount of money before the victims are provided with passwords to unlock their devices. Such technique is also known as ransomware. In 2019, there was an increase of 40% ransomware cases being reported by Singapore organizations, compared to 2018.

4 Cybersecurity readiness: case study of two small organizations in Singapore

As the first objective of this paper is to gain in-depth understanding of the causes for poor adoption of digitalization but proportion of cyberattack victims among the small organizations in Singapore, the authors performed in-depth review of the two small organizations, using case study method, to understand the root-causes behind the phenomenon in Singapore.

The knowledge gain from the study is expected to provide insights for better action plan to address the issues and to help successfully bring the small organizations up to speed on digitalization and cybersecurity.

For confidentiality, the two organizations are named as Organization A and Organization B.

4.1 Organization A

Organization A employs less than 25 staff and its annual revenue is less than US$3 million. Its annual surplus is less than US$0.5 million on average. Its main sources of revenue are the training courses and conferences it organises for professionals, mainly working in Singapore but there are a minority who are working in the South-East Asia countries.

Due to the COVID-19 pandemics, the government has capped the number of participants attending any single training and conferences at 5. This has adversely impacted Organization A, and it is expecting to incur losses in 2020. This has added challenges for it to pull through the crisis as its financial position was weak, even before COVID-19.

The board members of Organization A are mainly professionals working in the audit and risk management fields across various industries. As many of the board members are chief auditors or head of risk management, they are at the forefront of assisting their respective organization to strengthen cybersecurity.

Despite its weak financial resources, the staff members or Organization A constantly attend training sessions and seminars to keep abreast of latest development, include trends in digitalization, data analytics and cybersecurity. Therefore, the staff are aware of the trends and importance of digitalization and cybersecurity.

Although it is small, Organization A are led by professionals, who adopts a relatively open and consultative leadership style.

In the last few years, Organization A has embarked on automating its financial, human resource, and payroll systems. In 2020, it has upgraded its customer management system. These automation projects have instilled a change mindset among its staff. According to the most senior person in the organization, those automation projects have provided an excellent foundation for further change in the organization, she is confident that the staff are more ready to take on data analytics projects to better engage its customers. After automating its customer management system, Organization B is in the process of taking “baby steps” to embark on a data analytics journey.

During the interviews with the staff members, all of them have certain understanding of data analytics, while the majority of them view it as a necessary change going forward.

In addition, Organization A has engaged external professional firm to assess its standard of cybersecurity. The organization is in the process of rectifying the gaps identified. Based on the interviews with the board and top management, they view cybersecurity as an important initiative, such that they will “look for the fund to do it even if we do not have the money.” Organization A is fairly confident that its cybersecurity capability can protect the organization’s data to a large extend, although they are aware that no controls can be fool proof.

4.2 Organization B

Organization B employs about 140 staff and its annual revenue is in excess of US$20 million. On average, it has profit exceeding US$5 million per year, in the last 5 years.

In 2020, despite the impact of COVID-19 pandemics, it is on target to make a profit of approximately US$2 million, according to its revised budget.

At the end of 2019, the majority of the board members were entrepreneurs in their 70s. Data analytics is a term they rarely understood. As they grew up before the birth of personal computer, they have little training, and were reluctant to attend training, in technology and cybersecurity. The reluctance was raised in one of the correspondences with a regulator, who requested for the board's training plan. Two years after the request, the board had not provided the training plan to the regulator, which resulted in regulatory penalty.

Being Chinese entrepreneurs, the board members, in particular the board Chairman, adopted a relatively authoritative style. As the Chairman has little training and knowledge about data analytics and cybersecurity, there was no voice from the top to strengthen the organization to chart into these territories. Based on the observation and reading of archival documents, the board chairman has little understanding of the digitalization trends and has shown little interest to learn.

The top management members also have limited knowledge about cybersecurity. As a result, in the past few years, they did not engage professional firm to review and assess their cybersecurity capability. Consequently, the statutory auditors issued a management letter in early 2020 to urge the organization to perform an assessment of the cybersecurity capability.

Under the leadership of directors, who have little knowledge and interest to learn cybersecurity, the organization has undertaken little change management projects.

Table A below contrasts various factors for Organizations A and B.

Table A: Compare and contrast between Organization A and Organization B

	Organization A	**Organization B**
Annual revenue	<US$3 million	>US$20 million
Annual profit	<US$0.5 million	>US$5 million
Main revenue source	Training courses and seminar	Education services
Target market	Professionals	Secondary school students
Staff strength	<25	140
Board members' background	Professionals with strong exposures to governance, risk management and controls	Chinese entrepreneurs, mostly above 70 years old with little exposure to governance, risk management and controls. In addition, they have shown little interest to learn new skills
Staff exposure	Constantly updated on latest development in	Limited training and exposure to latest governance, risk

	governance, risk management and controls	management and controls. Rely on board members to give directions
Board culture	Consultative style where all the board members have equal voice	Authoritative style where the most senior guy (Board Chairman) has the loudest voice and the rest are expected to follow him
Exposure to change management	Went through big changes, in term of structure, systems and processes, in the last 3 years	Limited exposures to change from 2017 – 2019. Change in board members in 2020. The Chinese entrepreneurs retired and replaced by younger professionals in their 40s and 50s.
Awareness of data analytics	Most board and staff members are aware of data analytics, although most may not have the skills to execute data analytics, they know it is the important way to bring the organization forward	Some board members may aware of data analytics but the one with the loudest voice among them do not know about data analytics
Awareness of cyber-security	Fully aware of cyberthreats and have engaged a professional firm to review its security readiness	Limited awareness of cybersecurity. Statutory auditor raised a management letter point on the lack of cybersecurity assessment.

4.3 Insight drawn from the case studies

Based on the study of organizations A and B, it is interesting to note that financial resources are not the main driver behind slow adoption of digitalization and cybersecurity readiness. While Organization A has much weaker financial positions as compared to Organization B, it is in the process of adopting data analytics to provide better customer engagement. In addition, it has engaged a professional firm to assess its cybersecurity readiness. In contrast, although Organization B has more superior financial resources, it has no plan to adopt data analytics. It also needs the statutory auditor to nudge its management to engage professional firm to review its cybersecurity. This observation is somehow contrary to the findings in Sia (2018), who listed financial resources as the top challenge for a small organization in Singapore to adopt data analytics strategy.

The more advancement of Organization A to embrace data analytics and cybersecurity is mainly attributed to the awareness by its board and staff members, who have constant exposures and training in the two topics. On the other hand, the board and staff members of Organization B has little such exposures.

The situations in Organization B is made worse by its organization culture, which is authoritative. In some situations, the management may act as a sounding board to the board members by educating them on data analytics and cybersecurity strategies. However, the management needs a conducive and safe environment to voice their opinions. An authoritative style does not provide the management with the conducive and safe environment to do so. Therefore, with a board chairman who has little exposure and has shown great reluctance to attend training, the "ignorance' is deeply rooted throughout the entire organization, leading it to the poor state of adopting best practices for digitalization and cybersecurity. This demonstrates the importance of the tone from the top, and cybersecurity threats and risks must be managed from the boardroom (Lanz, 2014).

As one of the board members in Organization A has put it: "they (data analytics and cybersecurity) are important projects, we need to do to survive. If we do not have the money, let's go and look for the fund." The strong awareness in Organization A has led it to be the more advanced organization, between the two, to adopt digitalization and cybersecurity, despite having weaker financial resources.

5 Fight against cybersecurity threats

With the insights drawn from the two organizations, the authors are proposing key initiatives to help small organizations to embrace digitalization and cybersecurity in their pursuit for excellence.

5.1 Raising awareness at the top

There is an urgent need to communicate the importance of digitalization and cybersecurity to people, especially those serving in the senior roles and as board members of small organizations. This can be done through publicity and training. The Singapore government has put in tremendous effort to encourage Singaporeans and organizations to embrace digitalization and cybersecurity. However, the government cannot do it alone.

The government is of the view that cybersecurity is a collective responsibility of government, enterprises and individuals (CSA2, 2020). collaboration among these communities as well as academia is essential for digitalization and cybersecurity to be successful (CSA3, 2020).

Academia can play an important role in this aspect as it can design interesting courses to help people overcome the fear of the unknown and to step out of their comfort zone to attend the training. These training cannot be too technical but to demonstrate the "what" digitalization and cybersecurity can help. The objectives of the training is not to teach the board to ask technical questions, but to equip them with the knowledge to ask the right questions for the business and governance structure (Lanz, 2014).

5.2 Incentive and financial supports

Although the success story of Organization A demonstrates that financial resources are not the key obstacles, it cannot be generalized. There are other organizations who would need that extra help to fund the data analytics and cybersecurity projects. The government can either help to fund the projects directly, or to do so via certain self-help groups.

5.3 Peer support to keep abreast

As both data analytics and cybersecurity are relatively new areas, there are many learning opportunities, and organizations need to learn through trial and error during implementations. A common and easily accessible platform where like-minded organizations can gather and exchange experiences would help to facilitate more organizations to launch data analytics and cybersecurity projects.

5.4 Training to fill the shortage of talents

There is a severe shortage of talents in digitalization and cybersecurity. The issue is not unique to Singapore as it is estimated that the Asia Pacific region has a shortage of 2.15 million. The global shortage is estimated to be 3 million (CSA, 2019). The Singapore government is working with academia and businesses to train its workforce to meet the demand. In this regard, academia can help to train students with the right aptitude and skills to meet the demand of the industries.

5.5 Reinforcement - regulatory inspection, internal audit and external audit

With all the incentives provided, such as training, financial assistance, and peer group supports, there will still be some board members who are not engaged to tap on the resources to lead their organizations in the right directions. Therefore, there is a need to reinforce the implementation through inspection or audit, especially for cybersecurity. As a start, organizations can use their internal auditors to review its strategies and highlight weaknesses they noted (Lanz, 2014)

Without good cybersecurity, it is a matter of time that the organizations will be violating regulations, such as Personal Data Protection Act in Singapore, or General Data Protection Regulation if they are dealing with European customers. Therefore, auditors and inspectors have a duty to highlight the emerging risks.

In the case of Organization B, the statutory auditor has rightly raised a management letter point to highlight the potential risk to the board members, This demonstrates that auditors, and regulatory inspectors, have a significant part to play in enforcing organizations to strengthen their cybersecurity capability.

For organizations who continuously ignore the auditors' recommendation to review their cybersecurity, there should be penalties to deter such behaviours.

6 Conclusion

This paper has started by sharing the global and Singapore trends in adopting data analytics and cybersecurity strategies. It then focus on the situations in small organizations, where it has used two organizations based in Singapore as case study to draw insights. Based on the study, financial resources, while important, is not the most critical element for organization to embrace digitalization and cybersecurity. Instead, the awareness and willingness at the top of the house to embrace changes are the key to success. With this understanding, various stakeholders, including policy makers and academies, can play an important role to raise the awareness, provide training, and enforce the implementations.

The effort to successfully increase the pace of digitalization and cybersecurity adoption among the small organizations require a concerted effort of the entire communities, as nobody, including the government, can single handedly do it successfully (CSA, 2019).

7 Limitations and suggestions for future research

This paper is an exploratory research for small organizations in Singapore. It is performed using two small organizations as case study. While the characteristics, such as financial resource levels and compositions of the board members, are different in the two organizations, future research can be performed more comprehensively using bigger sample size or organizations with different characteristics. Studies can also be extended to include small organizations in other countries.

References

Alibaba Cloud. (2018). Digital transformation for SMEs. Alibaba Cloud: https://file-intl.alicdn.com/event/file/a38c87de-dac9-40d5-9f3c-fdeda2be8a15pdf?Expires=1557646750&OSSAccessKeyId=5JK9n2yWStiegAGj&Signature=Yb%2B3LL4C7M4tpGwUtnrBpK5cP%2BU%3D. Last accessed 2019/5/11.

Al-Moshaigeh, A., Dickins, D., and Higgs, j. L. (2019) Cybersecurity risks and controls. Is the AICPA's SOC for cybersecurity a solution? The CPA Journal, June 2019.

Al Zefeiti, S. M., & Mohamad, N. A. (2015). Methodological considerations in studying transformational leadership and its outcomes. International Journal of Enginering Business Management, 1-11.

Azorin, J. F. (2007). Mixed method in strategy research. Research methodology in strategy and management, 4.

Bada, M. and Nurse, J. R. C. (2019) Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security, Vol. 27, No. 3, pp 393-410.

Basias, N. P. (2018). Quantitative and qualitative research in business and technology: justifying a suitable research methodology. Review of Integrative Business and Economics Research, 7(1), 91-105.

Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Present scenario of IoT projects with security aspects focused. In Internet of Things: Digital twin technology, communications, computing, and smart cities; Farsi, M.,Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer Nature AG: Cham, Switzerland, 2019; pp. 95–123

CNA (2020) Channel News Asia Banking related phishing scams spike more than 2,500% in the first half of 2020. https://www.channelnewsasia.com/news/singapore/online-scams-increase-police-crime-social-media-impersonation-13053822. Last accessed on 2020/8/27.

Crowdcast Resource Center (2020) Learn what the European Union's General Data Protection Regulation (GDPR) requires and why cybersecurity is the key to compliance. https://www.crowdstrike.com/resources/crowdcasts/understanding-the-gdpr-and-how-it-will-impact-your-organization/?utm_campaign=dsa&utm_content=sea&utm_medium=sem&utm_source=goog&utm_term=&gclid=Cj0KCQjws536BRDTARIsANeUZ58FvYa07yeOoEOAiDWnHa5CdLOFBlJp5HcmazkD_0XgbaOy4Mh57j0aAqF0EALw_wcB. Last accessed on 2020/8/27.

CSA (2018) Cyber Security Authority of Singapore: Singapore Cyber Landscape 2017

CSA (2019) Opening speech by Mr Heng Chee How Senior Minister of State for Defence at the second Cybersecurity Awards and Gala Dinner. 8 Nov 2019. Last accessed 2020/8/16.

CSA1 (2020) Cyber Security Authority of Singapore: Opening speech by Mr Heng Chee How Senior Minister of State for Defence at the second Cybersecurity Awards and Gala dinner. https://www.csa.gov.sg/news/speeches/second-cybersecurity-awards-and-gala-dinner. Last accessed on 2020/8/15.

CSA2 (2020) Cyber Security Authority of Singapore: Singapore Cyber Landscape 2019

CSA3 (2020) Remarks by Mr David Koh, Chief Executive, Cyber Security Agency of Singapore, at the United Nations Security Council Arria Formula Meeting 2020.

Costley, C.; Elliott, G., Gibbs, P. (2010) Doing work-based research. SAGE pblication, 2010.

Dasgupta, M. (2015). Exploring the relevance of case study research. Vision, 19(2), 147-160.

DBS. (2018). 5 ways data analytics can help SME. DBS Business Class 11 September 2018. https://www.dbs.com.sg/sme/businessclass/articles/innovation-and-technology/data-analytics-can-help-SME Last accessed 2020/8/30.

DOS, Department of Statistics, Singapore. (2018). CEIC data. Retrieved from Singapore GDP per capita: https://www.ceicdata.com/en/indicator/singapore/gdp-per-capita

Gartner. (2018). Winning in a world of digital dragons. Stamford: Gartner Executive Programs.

Hair, J. F. (2018). Marketing research in the 21st centrury: opportunities and challenges. Brazillian Journal of Marketing, 17(5).

IBM (2020) Briefing paper: Companies are expecting more from digital transformation – and gaining more, too. Harvard Business Review.

Jahankhani, H., Al-Nemrat A., and Hosseinian-Far, A. 2014. Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator's Handbook. New York: Syngress, pp. 149-164.

Kerr, C., Nixon, A., & Wild, D. (2010). Assessing and demonstrating data saturation in qualitative inquiry supporting patient reported outcomes research. Expert Rev Pharmacoeconomics Outcomes Res, 10(3), 269 - 281.

Lambert, Y. (2020) Digital skills win in-house lawyers a seat at the table. The Financial Times. 7 August 2020.

Lanz, j (2014) Cybersecurity Governance: The role of the audit committee and the CPA. The CPA Journal, November 2014.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., and Kruschwitz, N. (2011) Big data, analytics and the path from insights to value. MIT Sloan Management Review, Winter 2011, Vol 52, No.2.

Lee, K. Y. (2000). From the third world to first, the Singapore story 1959-1999. Singapore: The Straits Times Press.

Lemieux, V. L, Gormly, B., and Rowledge, L. (2014) Meeting big data challenges with visual analytics. Records Management journal, 2014, Vol 24, No.2.

Lung, N. (2018). Singapore launches digital government blueprint to support its Smart Nation vision. 6 June 2018. https://www.opengovasia.com/singapore-launches-digital-government-blueprint-to-support-its-smart-nation-vision/ Last accessed on 2020/8/30.

Marrelli, A. F. (2007). Collecting data through case studies. Performance Improvement, 46(7), 39-44.

Microsoft and ASME. (2018). Singapore SMEs who embrace digital transformation expect to see average revenue gains of 26%. Retrieved 13 April, 2019, from https://news.microsoft.com/en-sg/2018/10/23/singapore-smes-who-embrace-digital-transformation-expect-to-see-average-revenue-gains-of-26-asme-microsoft-study/

Moore, C. (2011) The path to business process transformation. KM World, 2011, Vol 20, No.5.

OECD. (2017) Enhancing the contributions of SMEs in a global and digitalized economy. Meeting of the OECD Council at ministerial level, 7-8 June 2017. https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf Last accessed 2020/8/30.

Ong-Webb, G. A. (2017). Commentary: To benefit Singaporeans, Smart Nation must leverage big data, overcome privacy issues. 11 August, 2017. Channel New Asia: https://www.channelnewsasia.com/news/singapore/commentary-to-benefit-singaporeans-smart-nation-must-leverage-9114644. Last accessed 13 April 2019.

Oplatka, I., & Hemsley-Brown, J. (2004). The research on school marketing current issues and future directions. Journal of Educaton Administration, 42(3), 375-400.

Raelin, J. (2015) Action modes of research. A guide to professional doctorates in business and management. SAGE publication, 2015.

Ramchandani, N. (2017). Government making it easier for SMEs to adopt data analytics and AI. Retrieved 11 May, 2019, from https://ie.enterprisesg.gov.sg/Media-Centre/News/2017/10/Govt-making-it-easier-for-SMEs-to-adopt-data-analytics-and-AI--Yaacob

Shivkumar, S. (2019). All companies in Singapore must look to data to compete or risk becoming obselete. Retrieved 19 May, 2019, from Singapore Business Review: https://sbr.com.sg/information-technology/commentary/all-companies-in-singapore-must-look-data-compete-or-risk-becoming

Sia, N. C. (2018) The challenges for a small not-for-profit organization to embark on data analytics strategy. Amity Business Journal. Vol 5, No. 1, 18 August 2018.

ST ((2018) SingHealth cyberattack: how it unfolded. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html. Last assessed on 2020/8/23.

Tan, W. K. (1 November, 2016). Big data: Singapore's new economic resource. https://www.enterpriseinnovation.net/article/big-data-singapores-new-economic-resource-847989586. Last accessed 2019/4/13.

Tellis, W. M. (1997). Introduction to case study. The Qualitative Report, 3(2).

Teo, S. L. (6 June, 2013). Welcome address by Mr Teo Ser Luck, Minister of State for Trade and Industry at the SME Talent Programme. Partnership ceremony between institute of higher learning and trade associations and chambers: https://www.mti.gov.sg/Newsroom/Speeches/2013/06/Mr-Teo-Ser-Luck-at-the-SME-Talent-Programme--Partnership-Ceremony-between-IHLs-and-TACs. Last accessed 2020/8/30.

Yin, R. (1984). Case study research - design and methods. Beverly Hills: Sage Publications.

Yin, R. (2003). Case study research: design and methods (3 ed.). London: Sage.