INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 9, Issue 6, (2019) E-ISSN: 2222-6990

Establishing Information as Tangible Asset

[1]Dayang Ku Hidayah Awg Mohamad, [1]Nor Hanani Husain, [1, 2] Saiful Farik Mat Yatin,[1] Saidatul Akmar Ismail, [1]Hasnah Shuhaimi, [1]Shaharom Sulaiman, [1]Julieyana Jaris

[1]Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia

[2]Members of Advanced Analytics Engineering Center (AAEC),

UiTM

Email: farik@salam.uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i6/5970 DOI:10.6007/IJARBSS/v9-i6/5970

Published Date: 28 June 2019

Abstract

It is an idea that data, information and knowledge are different from intellectual capital. Data or information in a collection is more than knowledge. There is also no formality that intellectual capital is valuable organizational assets. However, intellectual capital is not only a set of information it does include expertise based on some degree of reflection. It is identified, managed and protected. In market view, the revolution of big data seems not giving impact to the development country such as Malaysia. Even there's highly usage of internet in communication through social media been adopted as Malaysian lifestyle. Study shows, Malaysia has busy traffic transaction of personal and business data and, the sensitive data stored in public cloud services exposed all the information to variety of risks in cyberspace. The revolution of information technology is never degreasing. As organizations are finding value in data, they realized the risk in handling information and the need of protection. In establishing information as tangible asset, this paper begins with cases of attack and security issues by applying analogy in framework. As the result, this paper suggests to ensure all the data, which can be, defined as tangible asset, with proven justification and acknowledge as a capital, will be protected by insurance policies with solid and concrete laws act.

Keywords: Information Management, Tangible Asset, Capital, Cyber Security, Data

Introduction

Big data hit the world like Tsunami. The explosion of data from the world's cyber revolution is becoming a hot topic as the world is now approaching the 4th Industrial Revolution (IR 4.0). The concept of the information is based on raw data, which consist of numbers, texts, and charts become meaningful data with knowledge after going through the data mining process. The big data break into four V's consists of Velocity, Variety, Volume and Veracity. Velocity refers to the measurement of the increasing units data. The variety of data types in the data such as photo, music, documents, numbers, texts and video. The volume vector is more and

more fill up data in the cloud and the data not decrease. The veracity is the degree to which data is reliable, useful and accurate. The issue of our topic is, no matter how valuables data nowadays, in our country, lots of parties look data as intangible, which opposite with the behavior of tangible, where the myth well said, tangible asset must be material, concrete, touchable, solid, visible, physical and real. The data also is an asset, which has highly value and need to be protected. This paper will discuss the idea of how data will become tangible and visible for Malaysia to start having awareness in protecting the business data towards the economic shift in developed countries from manual input to an intellectual and knowledge economy and the diffusion of technology from strictly the workplace into all aspects of personal and professional life.

Phenomenon

Today the world has undergone many developments in various aspects of life, especially the fastest growing technology. It has been a long time since humans have been using technology to assist their work in various areas of life, beginning from their role as a supporting tool to becoming a major tool for the execution of activities. The role of the internet can be the tools that have reached such a stage of development. Due to the enormous internet role in influencing the lives of human beings, a revolutionary idea emerged on the Internet of Things (IoT) and the Internet of Everything (IoE). For some internet users who daily basis use, for them it's hard to maximize the concepts of the Internet of Things (IoT) and Internet of Everything (IoE). It can be inferred as it sees its role in everyday life. However, it is generally concluded that IoE is not a technology tool that only acts as a remote control but a relationship between humans, data, and devices in an infinite dimension and can communicate with one another using the internet network. While IoT is a communication or communication system between devices that does not involve human intervention without the limitation of distance, time and space utilizing the internet network. The data exchanges and transaction happened in billions of bytes in every second.

Internet is no longer exclusive and it has become as new communication way, which contributes to trillions of data transaction within the cyberspace every day. Due to the nature of the internet that is adapted to our everyday world, then the internet is often referred to as cyberspace or virtual world. Just think, every 60 seconds, the world generates massive amounts of unstructured data 98,000+ tweets, 695,000 Facebook status updates, 11,000,000,000 instant messages, 168,000,000,000+ emails sent, and 1,820,000,000,000+ bytes of data created (HP, 2012). According to the research by MCMC, from 32 million peoples in Malaysia, 24.5 million users (76.9%) have access to Internet, and the others 7.5 million (23.1%) do not have access to the Internet (McKinsey, 2014). Whereby the smartphone is the main medium on how Malaysia accesses the Internet. There is 89.4% (21.9 million peoples) access their smartphone, compared to another medium such as laptop, netbook and PC desktop (McAfee, 2018) .The most amazing part, the Digital News Report 2017 found that Malaysians are the world's largest users of WhatsApp at 51 percent (Bernama, 2017).

Questions: How about the data security? Are we ready for data loss risk?

In competitive market, organization is force to implement continuous improvement. The process is guided from data which been managed and secure due to its value and sensitivity. When the improvement is data driven process it feeds decision maker to have a strong base

towards the year. High quality data able to lead good decision and proactive action, and the result will portray in their financial reports. Some organizations believe the challenge is about their massive data volumes. Others think the challenge is in the rapid rate of growth. Still others worry about the challenge handling the hack, data loss, disaster and cybercrime. As you can see above, the challenge is a perfect storm – facing all challenges simultaneously (HP, 2012) . To equip organization with infrastructures to manage their corporate assets and intellectual properties, third party services provider (MCMC, 2017) provides infrastructure as a service (IaaS) as platform. They also provide software as a service (SaaS) and platform as a service (PaaS). Organization shall choose whichever suit with their nature of business and risk management factors.

In lieu with that, in Asia-pacific, 63% of Sensitive Data consist of Personal Customer Info stored in public cloud services and 50% is payment card info (IT Best Practise, 2018) . Study shown, that Security Incidents Experienced in the Cloud persuasive 83%. The factor of the incidents may come from human lack of skills, not updated facilities and incomplete control over authority accessing the sensitive data (McAfee, 2018). World Economic Forum has reported USD3 trillion of impact due to cybercrime and this amount can be save if cybersecurity protection is well performed (MCMC, 2017).It also shown, from every one (1) from five (5) enterprises, they have experienced with advance persistent threat (APT) (ISACA, 2014; IT Best Practise, 2018) in which only one (1) can be trace to its resource. This explained that globally, organization still under prepared or unprepared for advanced security threat despite awareness activities via media and education. Data security and protection is a real business. In Malaysia, relevant law which covered various issue with data related either its commercial, non-commercial or crime has been established (McKinsey, 2014) . It has outlined enforcement agency as well.

Table 1: Relevant law in Malaysia related with content

Type of offence	National Laws	Enforcing Agencies
Sedition	Sedition Act 1948	Royal Malaysia Police (PDRM)
Threats to National Security	Penal Code	Royal Malaysia Police (PDRM)
Fraud/Finance/Trade	Companies Act 1965	Companies Commission of Malaysia (SSM)
	Financial Services Act 2013	Bank Negara Malaysia
	Direct Sales Act 1999 Consumer Protection Act 1999 (online sales & purchase transaction)	Ministry of Domestic Trade, Cooperative and Consumerism (KPDNKK)
	Capital Market & Services Act 2007	Securities Commission Malaysia (SC)
	Electronic Commerce Act 2006	Ministry of Domestic Trade, Cooperative and Consumerism (KPDNKK)
	Penal Code Section 420	Royal Malaysia Police (PDRM)
Copyright	Copyright Act 1987	Ministry of Domestic Trade, Cooperative and Consumerism (KPDNKK)
Defamation	Penal Code Defamation Act 1957	Royal Malaysia Police (PDRM)
Gaming/Betting	Common Gaming Houses Act 1953 Betting Act 1953 Pool Betting Act 1967	Royal Malaysia Police (PDRM)
Threats to Life/Property	Penal Code	Royal Malaysia Police (PDRM)
Hacking	Computer Crime Act 1997	Royal Malaysia Police (PDRM)
Personal Data	Personal Data Protection Act	Department of Personal Data Protection

Case study on software liability implies that variety of information that can be accessed via electronic has increased the thread of safety in various aspects. It is not only the safety of system itself, but the safety of human while exposing them with the system (Laws Of Malaysia, 2010). The lack of physical data eventually will engender a higher expectation of reliance and thus safety on electronic access system (IT Best Practise, 2018). Where dependence on such system become the norm, it is difficult not to expect more stringent rules to be applied by organization. In the context of the complexity of electronically accessed system, expert system and other increasingly similar ones, strict liability assures compensation to victims, which is also justifiable on moral and practical grounds (MyCyberSecurity, 2018).

The Cyber Act being implemented

The Department of Personal Data Protection (JPDP) is an agency under the Ministry of Communications and Multimedia (KKMM). This Department was established in May 16, 2011 after the Parliament passed the Personal Data Protection Bill 2009, the main responsibility of this Department is to enforce and regulate PDPA in Malaysia. PDPA focuses on the processing of personal data in commercial transactions and avoid of misuse of personal data. Personal Data Protection Act (PDPA) came into force in 2013, and the penalty for non-compliance is anywhere between RM100, 000 to RM500, 000 and/or 1-3 years of imprisonment (Jabatan Perlindungan Data Peribadi, 2018) .

Finding

Malaysia insurance policy still looks at data as intangible asset, which become difficult to determine, what a good insurance risk is. Only three (3) insurance companies offer cyber insurance in Malaysia offers policy for data. As of December 2017, there's 60 cyber insurance

policies deployed in Malaysia. For business data insured, each million ringgit (RM) of insured value, incurs a premium of RM10, 000 per annum whereby too low compare to the value of the data itself as an asset. A database of a manufacturing plant, which has, operates more than 10 years, for example will have massive historical data which are vital to the organization.

Most of insurance policies give clarification that it is difficult for the insurance company to place premiums that can be recovered on intangible data for the factors of data loss, as these losses are not hard and fast definitions. They are focusing in providing infrastructure of the business with empty box. For example, data center damage due to fire, insurance company provides data center equipment facilities including related licenses. When data restoration is in practice, it is out of scope for insurance. The lines keep blurring and changing, especially these days, as cybercriminals get more creative about how they infiltrate and what they take. However, the loss of business data cannot be taking for granted; authorities still accept data loss cases as a crime.
Christopher and Lee Ong: Deepak Pillai in their The International Comparative Legal Guide to: A practical cross-border insight into cybersecurity work 1st Edition Cybersecurity 2018 do write the collection of law acts related to Malaysia cyber law. To date, since publication of this Guide, there is no single legislation in Malaysia in respect of cybersecurity (Pillai, 2017) . So, there is a lot that is still left unprotected. (Global Legal Group, 2017) . The legal officer base in Putrajaya Attorney General, said that only one case related to business data had been forward to court and the case still in process which the claim on intangible asset in Malaysia consider as rare and the loose in the act.

Data as an Asset
Data is life blood to organization. Thus, it is vital to the business continuity and operation. It must be protected from elimination, destruction and loss. “Value has a value only if its value is valued “– Bryan G. Dyson (the CEO of Coca-Cola, 1988-1994). Analogy can be associated between value and asylum protection given is deposit in bank and deposit insurance. Every bank in Malaysia subjected to Central Bank of Malaysia Act to operate (Laws Of Malaysia, 2009). Government protect depositors against the loss of their deposits via Deposit Insurance system. To enjoy this facility, the bank must be a registered member of PIDM (PIDM, 2018).

The existing of PIDM is to reinforces and complement regulatory. PIDM also supervise frameworks by providing risk management in financial system. They are protecting depositors from the loss of deposit by reimbursing as soon as possible. It’s a good image for our Malaysia’s financial system (MCMC, 2018) .

Data has value when we give value from requirement and compliance that derives from good governance. How we value our data? The history is in intangible asset assessment, a metric developed by comparing market capitalization to replacement value of assets. For a high-growth technology company in order to sustain and compatible in the market, the most valuable data is human capital. This significant intrinsic value is in the know-how and innovation of the employee. Human capital is the term for the collective capability, knowledge and skills in which creates the value in long term

Thus, we have policies to cover our business. Disaster recovery plan will help setting up business in the event of disaster. The policy shall also include related rules and regulations by law for example OHSAS(MyCyberSecurity, 2018) .The data may not give any meaning, such as individual name without surname, but what if the data include the full name, email, phone number, identity card number and address, it will become aggregating data. Variety of information turns into rich dataset which much stronger digital compound and makes the data much value information. The data shall be protected regardless of personal data, but the whole data in business which ever stored in the cloud, data server, database, local desktop or other devices. Whatever data which giving meaningful to the irresponsible parties will manipulate the data for bad sentiment or worse do other unpredictable crime.

When facility and equipment are well developed and govern by skilled personnel, as a standard practise of risk management, we will get insurance for our data centre and all IT equipment. In Malaysia, as of April 2018 only three insurance companies declare they have policy for data protection. However, the policy didn't cover the business data. In the event of disaster, insurance covered the setup of new place infrastructure and equipment's. We will get the licenses and application but with no data. It's like an empty building complete with facility but without business. If the backup data failed to restore or can't be use to run the business in relation with the disaster, we have no coverage. The data for 20-30 years of business is gone despite investment made and value given.

Conclusion

Malaysia shall be moving forward, to practice with respect data, risk mitigation shall include value of stored data, establish legal act to protect business data and impose insurance coverage. Europe Awareness on Protecting Data and Insurance Policies for Data Loss since 2005, speech by the President of the Italian Data Protection Authority presenting the 2005 annual report to Parliament - July 7, 2006. The speech contents, the direction of the people and the awareness of European on data protection authorities that re-affirmed data protection is a fundamental feature of societies with the various stages of today's culture and civilization (President of the Italian data protection authority) as computing technology brought above the revolution in information technology (PIDM, 2018) . Nowadays a variety of information can be accessed electronically. Mechanical and increasing instances of human mediated functions are taken over by digital technologies. Legal rules developed over a period of time and applying to different sets of conditions remain. However, the essence of legal rules still remains valid, only that it could be slow to respond when novel situation arises. Informational content accessible in electronic form is an example. Negligence rules requiring cumbersome methodologies may not provide justice in the modern setting. Various quarters including government, corporate bodies, NGOs should play a role in empowering cyber-law in protecting data rights while bringing data in the realm of reality to be valued as valuable and insurable assets in Malaysia. The government needs to examine the essence of the data itself that is capable of generating a national economy, today's world sees who controls the data will dominate the world. This is because the current situation of data can be a milestone in anticipation of the profitable gain within a year, three years or, nine years and so, therefore, it is highly recommended that data be provided with insurance cover similar to *Perbadanan Insurans Deposit Malaysia* (PIDM) protecting bank account. The state's credibility in empowering insurance coverage on data primarily for business data, demonstrates the

economic stability and reliability of outside investors, particularly those related to cyber investment and technology-based businesses to invest in the country. Hence, there needs to be awareness about data protection and related acts not only on personal data but as a whole to all sensitive data. The enforcement from the government to declare business data as tangible asset will assist the review law and act by the prior lawmaker to be implemented in Malaysia. All embracing and complex products in the informational context require perhaps a more vigorous approach. Strict liability regimes are thus justifiable in these situations, especially when computer access systems are increasingly being used and thus affecting more and more lives. It is appropriate to generate greater care, responsibility and safety. Perhaps it is time for a suitable general approach to information technology could point the way forward. Meanwhile, strict liability laws should be imposed to provide safer systems to prevent injury that are presently difficult to prove in the circumstances or to provide remedies in the event of injury and not be delayed until the day when it may have to be written 'in the blood of injured victims'. (Yong, 2007) Only then, the law has holistic guidelines which covered data as tangible asset, methods of asset management, environment and people operate the system.

Acknowledgement

This paper was partially funded by:

1. Conference Support Fund, Institute of Graduate Studies (IPSis, UiTM)
2. Management Fund, Faculty of Information Management, UiTM

Corresponding Author

Saiful Farik Mat Yatin. Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia

References

Erickson, S., & Rothberg, H. (2014). Big Data and Knowledge Management: Establishing a Conceptual Foundation. *The Electronic Journal of Knowledge Management*, 108-116.

Bernama. (2017). *Malaysians are world's largest WhatsApp users*. Retrieved from New Straits Times Malaysia: https://www.nst.com.my/lifestyle/bots/2017/09/278936/malaysians-are-worlds-largest-whatsapp-users

Global Legal Group. (2017). The International Comparative Legal Guide to Cyber Security 2018.

HP. (2012). *Information Optimization Harness The Power of Big Data.* HP Business White Paper.

ISACA. (2014, April). ISACA's 2014 APT Study. *ISACA*.

IT Best Practise. (2018). UNIVERSITY OF NEBRASKA–LINCOLN. Retrieved from https://its.unl.edu/bestpractices/server-administration

Jabatan Perlindungan Data Peribadi. (2018). *Department Of Personal Data Protection*. Retrieved from http://www.pdp.gov.my/index.php/en/

Laws Of Malaysia. (2009). Central Bank of Malaysia Act 2009. In *Laws of Malaysia Act 701.*

Laws Of Malaysia. (2010). Personal Data Protection Act 2010. In *Laws Of Malaysia Act 709.*

McAfee. (2018, April 16). *1-in-4 orgs using public cloud has had data stolen*. Retrieved from https://www.helpnetsecurity.com/2018/04/16/public-cloud-stolen-data/

McAfee. (2018). *McAfee study: 1-in-4 organisations using Public Cloud has had data stolen*. Retrieved from https://www.digitalnewsasia.com/business/mcafee-study-1-4-organisations-using-public-cloud-has-had-data-stolen

McKinsey. (2014). Increased cyber security can save global economy trillions. *World Economic Forum*.

MCMC. (2017). MCMC Internet Users Survey .

MCMC. (2018). *Malaysian Communications and Multimedia Commision* . Retrieved from https://www.mcmc.gov.my/

MyCyberSecurity. (2018). *Data Recovery Services* . Retrieved from My Cyber Security Clinic: 11. http://cybersecurityclinic.my/index.php/joomla-pages-iii/blog-layout/26-data-recovery-services.html

PIDM. (2018). *Perbadanan Insurans Deposit Malaysia*. Retrieved from http://www.pidm.gov.my/en

Pillai, D. (2017). The International Comparative Legal Guide to Cyber Security 2018. Retrieved from https://www.christopherleeong.com/media/2883/cyb18_chapter-17_malaysia.pdf

President of the Italian data protection authority. (2006, July 7). Speech by the President of the italian data protection authority presenting the 2005 annual report to Parliament. *Garante Privacy*. Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1332401

Yong, P. (2007). Software Liability . *Malayan Law Journal Articles*.