Big Data Management & Security Threat under OBOR

Dr. Gryphon Sou
Visiting Professor
City University of Macau, Macau Special Administrative Region (MSAR)
GryphonSou@cityu.edu.mo

ABSTRACT

Big Data is characterized by its four features: (1) Volume, (2) Velocity, (3) Variety and (4) Veracity. Information security and data protection issues are magnified by these features of Big Data. Therefore, traditional security mechanisms, which are tailored to securing small-scale static data, are inadequate. Either private or public sector should be ready for Big Data management and face its inherited security threat. This Paper studies the characteristics of Big Data and review the Cyber Attack in the last decade. With reference to ISO 27001: 2015 and best trade practice, this Paper also proposes security solutions for possible Cyber Attack on Big Data.

Keywords: Big Data, Cyber Attack, Information Security; Ransomware; Security Solution.

1. Introduction

Data is said to be the new gold of this digital age (Goldsmith, 2017). The term Big Data refers to the massive amounts of digital information companies and governments collect about us and our surroundings (CSA, 2012). It has become crucial for business organizations and government bodies to gain actionable insights for policy making, efficiency enhancement and community engagement.

Liedtke (2015) quotes that Big Data represents a situation where we have significantly more data than usual, for instance, a database containing 50,000,000 rows and 75 columns – terabytes. This is not a useful definition because traditional statistical methods can still be used and it does not adequately reflect what is happening in the data management.

Liedtke (2015) also quotes that Big Data represents a situation involving a large amount of data consisting of multiple data types sometimes arriving real-time from multiple sources requiring exploratory data analysis and integrative analytical methods for problem-solving and problem-discovering. This is a more useful definition consistent with what is happening in the Big Data management and it suggests the need for new management techniques and skills.

1.1 Big Data Value

Big Data is characterized by its four features: (1) Volume, (2) Velocity, (3) Variety and (4) Veracity (Linuxpilot, 2015). Information security and data protection issues are magnified by these features of Big Data (Figure 1). Therefore, traditional security mechanisms, which are tailored to securing small-scale static data, are inadequate. Either private or public sector should be ready for Big Data management and face its inherited security threat.

On October 28, 2016, China issued "Belt and Road Initiative Big Data Report 2016" in Beijing. This first book of Big Data was supervised by the General Office of the Leading Group for advancing the building Belt and Road Initiative, released by the State Information Center (SIC) and published by Commercial Press. One-Belt-One-Road (OBOR) countries should be ready for Big Data management and malicious Cyber Attack. Otherwise, the hackers may deprive the value of our Big Data by means of malware.

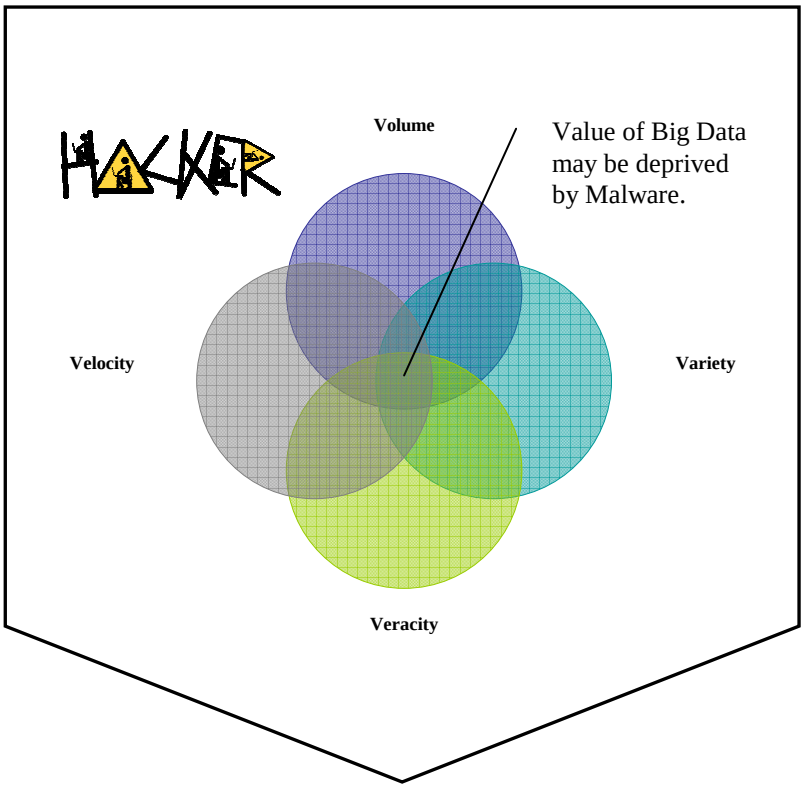

Figure 1: Value of Big Data to be protected (Source: Sou, 2017)

2. Empirical Case Study

2.1 Research Methodology

This Paper studies the characteristics of Big Data and review the Cyber Attacks in the last decade. Author of this Paper is a registered United Kingdom Information Technologist and Diagnostic Engineer. Applying diagnostic engineering skills and expert opinion, he tries to analyze the security threat of the contemporary information technology infrastructure.

With reference to ISO 27001: 2015 and best trade practice, this Paper also proposes security solutions for possible Cyber Attack on Big Data. Benchmarking business organizations and government departments in some countries, the author proposes information technology solutions to address security issues surfaced in the prevailing Cyber Attack.

2.2 Case Study 2016

Information Systems Audit and Control Association (ISACA) is an independent, nonprofit, global association. It is engaged in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA once conducted a global survey in 129 countries. The Survey revealed that only 38% of respondents were prepared for a Cyber Attack. Ironically, 83% of respondents believed that Cyber Attacks are amongst the top three threats at the corporate level.

2.2.1 Asian Government Cases

In 2016, two agencies and four functional departments of the Government of Hong Kong Special Administrative Region respectively encountered Cyber Attacks:

✧ Customs and Excise Department
✧ Department of Health
✧ Food and Environmental Hygiene Department
✧ Marine Department

One of the foregoing government departments has implemented ISO 27001 for 16 years. It maintains the Quality and Information Security Management System (QSS) which meets the requirements of the ISO 9001:2000 and ISO 27001:2005 standards. However, it becomes a victim of Cyber Attack (Figure 2).

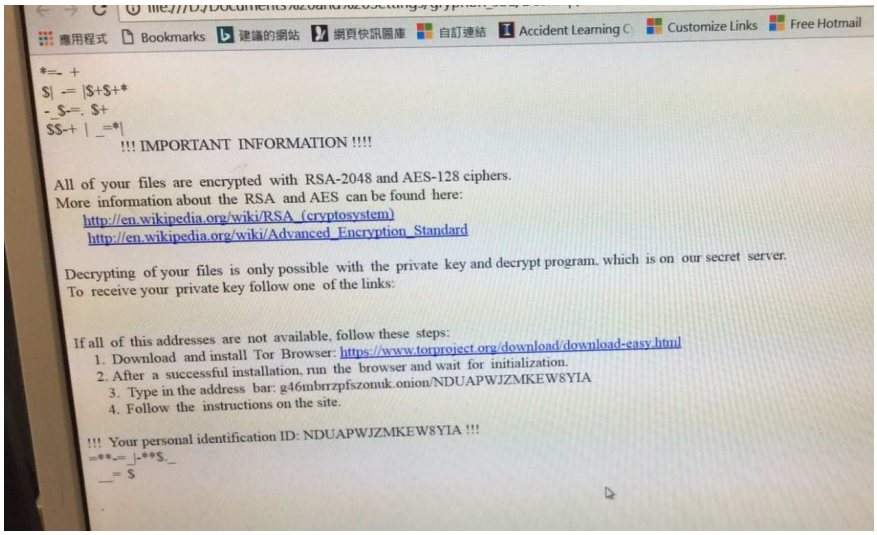

Figure 2: Cyber Attack on a Government Department (Source: Sou, 2017)

Symantec.

***Scan type* or Symantec Endpoint Protection Detection Results**

When the client does not detect any viruses in scanned files, the progress bar shows that the scan is complete.

If the client detects a virus during the scan, then the infection details appear in the results list.

Note: If the Symantec Endpoint Protection client for Windows detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages. The scan restarts and uses Insight lookups.
See About the aggressive scan mode.
See How Symantec Endpoint Protection uses reputation data to make decisions about files.

Table: Infection details

Option	Description
Icon	The icon that indicates whether or not a file or risk is still a threat. A green check mark indicates that a risk or file is no longer a threat. A red "x" indicates that a risk or file is still a threat.
Filename	The name of the infected file. **Note:** The language of the operating system on which you run the client might not be able to interpret some characters in virus names. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some Unicode virus names might contain double-byte characters. On those computers that run the client on an English operating system, these characters appear as question marks.
Risk	The name of the detected risk. You can click on the risk name to display more information about the risk on the Symantec Security Response website.
Action	The action that the client performed on the risk, if any.
Risk Type	The category of the detected risk.
Logged By	The type of scan that detected the risk.
Original Location	The path to the folder where the client detected the risk.
Computer	The name of the computer where the client detected the risk.
User	The name of the active user when the client detected the risk.
Status	The state of the detected file.
Current Location	The path to the folder of the infected file if it remains on the computer.
Primary Action	The configured first action for the detected risk.
Secondary Action	The configured second action for the detected risk.
Action Description	An explanation of the action that the client performed on the detected risk, if any.
Date and Time	Displays the date and time that the client detected the risk.

Figure 3: Scanning Software of the Victimized Government Department (Source: Sou, 2017)

During and after a Cyber Attack by the end of 2016, its firewalls and virus scanning software (Figure 3) could not alert the users. The malware attacked the Hard Disk of a terminal with Universal Serial Bus Portable Drives and so forth SHARED Folders through the departmental and local network. Such situation surfaced the vulnerability of its existing information technology infrastructure. The malware unknowingly circumvented regular scanning of its Symantec Endpoint Protection software and other information technology measures in place.

Apart from four government departments, two Hong Kong government agencies were attacked in August 2016 too. The China-based group APT 3 targeted them with "spear-phishing" attacks, in which e-mails with malicious links and attachments containing malware were used to access their computer networks. An American information technology firm was subsequently hired to identify attackers.

The government agencies remained anonymous to avoid shining a spotlight on the victims. The Office of Government's Chief Information Officer (OGCIO) confirmed that it had been informed about the hacks. "Relevant security measures had already been put in place to block the suspicious e-mails," it said in a statement. "So far, there is no security incident report from the two concerned departments (agencies)."

2.2.2 Healthcare Industry Cases

Ransomware is not a new malware in Cyber Attack but its growth throughout 2016 has made its prevalence known around the world. Organizations in the private and the public sectors were victimized. A July 2016 report revealed that the healthcare industry was attacked significantly harder by Ransomware than any other sector – 88 percent of attacks hit hospitals (Dietschye, 2016 & Green, 2016).

Becker's Hospital Review (2016) reported that 12 healthcare-related Ransomware Attacks in six months. With reference to Solutionary's Security Engineering Research Team Quarterly Threat Report Q2/2016, 94 percent of attacks on healthcare organizations are linked to a specific variant of malware called Cryptowall.

In February 2016, a Los Angeles hospital paid 40 Bitcoins of digital currency (USD17,000) to Ransomware hackers (The Guardian, 2016). Federal Bureau of Investigation often discourages victim to pay the ransom as it would encourage hackers. Hackers always customize the ransom for each victim and set them just low enough to seem palatable, if a bit painful (The Guardian, 2016). In the Los Angeles case, the President and Chief Executive of the Hollywood Presbyterian Medical Center said, "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom. … In the best interest of restoring normal operations, we did this." (Yadron, 2016).

In May 2016, Kansas Heart Hospital became the second healthcare organization in America which publicly stated that it had paid the ransom. Hackers collected ransom from the Hospital but did not unlock all the data and then demanded more money. President of Kansas Heart Hospital told the media that the first ransom was "a small amount" (Siwicki, 2016). However, he declined to pay the second ransom as it was not a wise move. He added that his hospital was aware of the looming ransomware threat and had a plan in place, highlighting that many organizations do not really know how to respond to a Cyber Attack.

3. Results & Analysis

3.1 Big Data Security Challenges

Cloud Security Alliance (CSA) highlighted the top ten Big Data specific security and privacy challenges (CSA, 2012). Experts of CSA interviewed the Alliance members and surveyed security practitioner-oriented trade journals to draft an initial list of high-priority security and privacy problems. Studied published research, CSA experts arrived at the following top ten challenges (CSA, 2012):

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transaction logs
4. End-point input validation or filtering
5. Real-time security or compliance monitoring

6. Scalable and compostable privacy-preserving data mining and analytics
7. Cryptographically enforced access control and secure communication
8. Granular access control
9. Granular audits
10. Data provenance

To study information security threat, we shall focus on Item 5. Real-time security monitoring has always been a challenge, given the number of alerts generated by the security tools. These alerts lead to many false positives, which are mostly ignored or simply "clicked away", as data users cannot cope with the shear amount (CSA, 2012). This problem might even increase with Big Data, given the 4 Vs (Volume, Velocity, Variety and Veracity) of data streams.

However, Big Data technologies might also provide an opportunity, in the sense that these technologies do allow for fast processing and analytics of different types of data. Which in its turn can be used to provide, for instance, real-time anomaly detection based on scalable security analytics (CSA, 2012). Security screening and risk analysis should keep pace with the dynamic analysis of Big Data.

With real-time security monitoring, we try to be notified at the moment a Cyber Attack takes place. In reality, this will not always be the case. For instance, new attacks, missed true positives are difficult to be monitored. For investigation of a missed Cyber Attack, we need audit information. This is not only relevant because we want to understand what happened and what went wrong, but also because of compliance, regulation and forensic reasons. In this regard, auditing is not something new; but the scope and granularity might be different and should keep pace with the trend of information security threat.

3.1.1 Advanced Persistent Threats

Gartner (2012) said, "Organizations face an evolving threat scenario that they are ill-prepared to deal with … advanced threats (Figure 4) that have bypassed their traditional security protection techniques and reside undetected on their systems.". Since 2012, Advanced Persistent Threats (APTs) have become more prevalent. APTs targeted at critical infrastructure. They were persistent and difficult to be detected. APTs spread via LAN as well as USB.

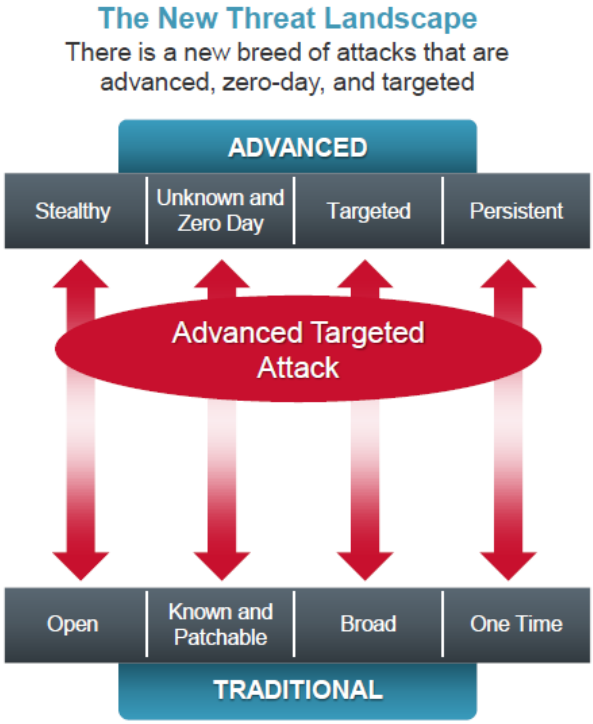

Figure 4: Contemporary Information Security Threat (Source: FireEye, Inc., 2012)

Nowadays, APT utilizes advanced techniques and/or malware that is unknown, targeted, polymorphic, dynamic and personalized. It uses zero-day exploits, commercial quality toolkits and social engineering. It often targets IP, credentials and often spreads laterally throughout network. Ransomware is a typical APT.

Facing the new threat landscape, typical security architecture (Figure 5) failed to tackle. In other words, existing threat intelligence is lack of automation from the basic threat intelligence to threat fingerprint.

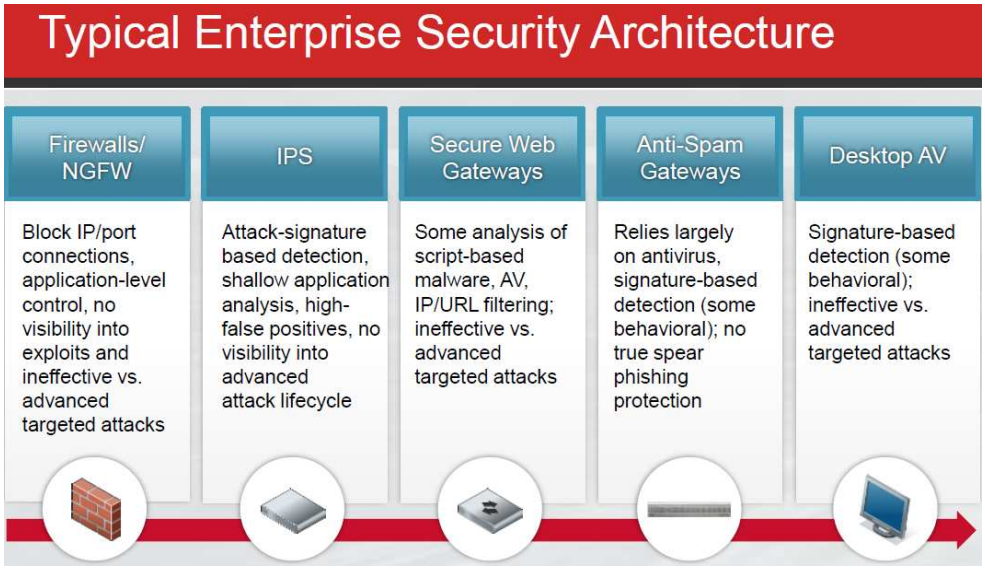

Figure 5: Typical Enterprise Security Architecture (Source: FireEye, Inc., 2012)

The above illustration surfaces that typical security architecture in most information technology infrastructure is inadequately tackling APT like Ransomware. Terminals have access to the internet (hyperlinks) and internet-mail or web-mail servers. They are naturally exposed to APTs. Though ISO 27001/2:2013 is a good global standard to follow for information security and privacy (Villanustre, 2014), data users habitually use their "own" USB Thumb Drives on the office terminals as some brands of Portable Drives can cheat the corporate computer systems. Regardless of rules and regulations, a Whitelist Portable Drive System easily collapses within an organization with mass data users.

3.2 International Standards for Information Security

Humphreys (2015) of International Organization for Standardization (ISO) emphasizes, "To ensure security in today's digital landscape, all organizations, irrespective of size should put in place a management framework as a starting point to manage cyber risks. ISO/IEC 27001 was designed to help organizations do just that. The standard is the world's 'common language' when it comes to assessing, treating and managing information-related risks.".

ISO/IEC 27000 series were revised in 2015. They formed part of the ISO/IEC 27001 "cyber-risk toolbox" to help keep information security threat in check (Lazarte, 2015). To name a few but not all, the following international standards are of referential value in Big Data management and information security threat mitigation.

3.2.1 Integrated Solutions for Services (ISO/IEC 27013)

More organizations are choosing to combine an information security management system (ISO/IEC 27001) with a service management system (ISO/IEC 20000-1). An integrated system means an organization can efficiently manage the quality of its services, handle customer feedback and solve problems, whilst keeping information (data) safe.

ISO/IEC 27013 offers a systematic approach to facilitate the integration of an information security management system with a service management system. It results in lower implementation costs and avoids duplication efforts in certification audit.

3.2.2 Detecting and Preventing Cyber Attacks (ISO/IEC 27039)

How can organizations detect and prevent cyber intrusions to their networks, systems and applications? Best trade practice shows that they must be able to know when and how an intrusion occurs. They should also be ready to identify what vulnerability was exploited and what controls should be implemented to prevent recurrence of similar intrusion in the future. One way to do this is through an Intrusion Detection and Prevention System (IDPS) (Figure 6).

ISO/IEC 27309 gives guidelines to prepare and deploy an IDPS, covering such crucial aspects as selection, deployment and operation. The standard is particularly useful in today's market where there are many commercially available and open-source IDPS products and services based on different technologies and approaches.

3.3 Findings

In short, internet access, email and unauthorized portable drives imposed risks to an organization. APTs possible damage to its information technology infrastructure and Big Data could be disastrous. In such circumstances, we should consider addressing APTs in the most realistic manner. Considering multiple stages of an Attack Cycle and Multi-Flow Virtual Execution (MVX), the Author finds that there is actually information security solution for APTs.

Benchmarking other victimized Government departments and business organizations, the Author appraises FireEye Advanced Threat Protection Architecture. Diagnosing FireEye architecture and hardware/software engineering, its concept of "behavioral" Malware Protection System (MPS) as an IDPS is viable. Its inline blocking and quarantine available across MPS portfolio can:

✧ block inbound zero-day web attacks
✧ block multi-protocol call-backs
✧ quarantine malicious zero-day emails
✧ quarantine malicious zero-day files
✧ mitigate risk of data exfiltration
✧ provide highly actionable information for timely incident response.

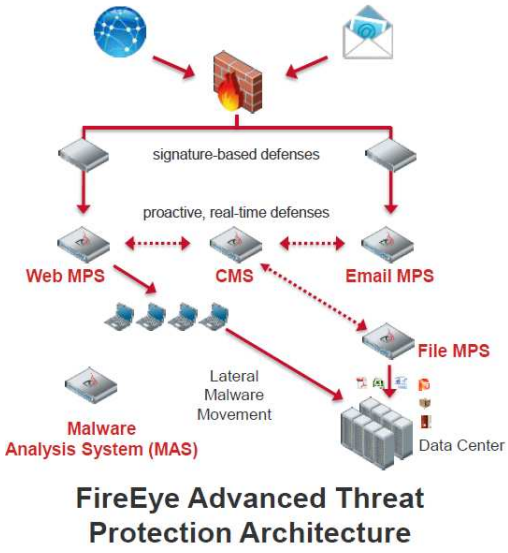

Figure 6: Intrusion Detection and Prevention System (Source: FireEye, Inc., 2012)

4. Conclusion and Recommendations

This Study reveals that MPS hardware can tackle information security threat. Capacity of hardware can cater for the information technology operational needs (100 users @ 20 Mbps – 10,000 users @ 1 Gbps) of Small-and-Medium Enterprise to transnational enterprises. An American hardware manufacturer has global credentials. Its product has the following key features:

✧ Detect inbound 0-day and customs malware via virtual machine analysis
✧ Track outbound call-backs and subsequent malicious payloads
✧ Extremely accurate detection with near-zero false positive

In America, it also supplies 10-Giga native solution. If other global hardware manufacturers are supplying the same or kindred MPS, they are also of referential value to prospective users. In conclusion, this is a viable information security solution to rebut the fallacy of *"even the most powerful scanning software fails to detect newest or customs-made virus or malware"*. That is to say … we need software plus hardware in order to counter APT and preserve the value of our Big Data (Figure 1).

References

APPLE DAILY (2016) Two Computer Terminals of the Center for Food Safety Hong Kong attacked by Hackers. *Apple Daily*. Hong Kong.

CHEUNG, K. (2012) FireEye, Proactive Approach to Advanced Persistent Threat (APT). Hong Kong, iCON Business System Ltd.

CHINA.ORG.CN (2016) Book Launching of "Belt and Road Initiative Big Data Report 2016". Beijing, General Office of the Leading Group for advancing the Building of Belt and Road Initiative.

CHOI, K. L. (2017) ICON Expert explaining Hints of Anti-APT. Hong Kong, Linuxpilot.

CSA (2012) Top Ten Big Data Security and Privacy Challenges. New York, Cloud Security Alliance.

DIETSCHE, E. (2016) 12 Healthcare Ransomware Attacks of 2016. *Becker's Health IT & CIO Review***,** 2-4.

EY (2017) Analysis of the "One Belt, One Road" Initiative - Telecommunications and Aviation Sectors. *China Go Abroad*.

GOLDSMITH, S. (2017) Experience Sharing by Professor Stephen Goldsmith, Harvard University. *Seminar on Data-Smart Governance - Connecting with the Communities*. Hong Kong, CSTDI.

GREEN, M. (2016) Hospitals are hit with 88% of All Ransomware Attacks. *Health Information Technology***,** 2-3.

SGS. (2008) HK Customs: The First Department of HKSAR to implement ISO 27001. Hong Kong, SGS Group.

HIT CONSULTANT (2016) Healthcare Ransomware: Why Providers should not pay the Ransom. IN OUT THOUGHT LEADERS (Ed.) Chicago, HIT Consultant Media.

--- (2017) Ransomware leads the Way in 2017's - Predicted Rise in Health Data Attack. IN OUT THOUGHT LEADERS (Ed.) Chicago, HIT Consultant Media.

LAZARTE, M. (2015) Security Toolbox protects Organizations from Cyber Attack. London, International Organization for Standardization.

LIEDTKE, C. A. (2015) Big Data Quality Management: A Glimpse into the Future. *Minnesota Section of American Society for Quality*. Minnesota, USA, MNASQ.

LINUXPILOT (2014) iCON helps STDM to build Private Cloud for Enhancement of Collaboration and Decision Making. Macau, Sociedade de Turismo e Diversoes de Macau, S.A.

--- (2015) Big Data help Enterprise making Profit? Stop and Think before Use. *Linuxpilot.*

--- (2015) HP with Red Hat using Innovative Technology to boost Real Time Big Data Analysis. *Linuxpilot.*

--- (2017) Welcoming futuristic Hyper-Converged Infrastructure - Nutanix with iCON boost Lean Enterprise Computing. Hong Kong, iCON.

MAK, K.-L. (2015) Xynergy helps Retail Industry applying SAP HANA - Integration of Big Data Analysis with Automatic Intelligent Vending Machine. *Business Quotient Journal,* 55**,** 6-7.

ORIENTAL NEWS (2016) System being hacked for 9 Days - 17,000 Data Files of the Department of Health being compromised. *Oriental News.* Hong Kong.

SINGTAO NEWS (2016) Hackers attacked Computer System of the Marine Department for Ransom. *Singtao News.* Hong Kong.

SIWICKI, B. (2016) Ransomware Attackers collect Ransom from Kansas Hospital, don't unlock all the data,

then demand more money. *Healthcare IT News.* Kansas.
IBS. (2014) iCON Quality Network and Security Services entrusted by Government Departments and brings Innovative Technology. *Business Quotient Journal***,** 1-4.
SOU, G. (2017) A proposal improving work-related Information Technology Security. Hong Kong, Customs and Excise Department.
TWEED, D. (2016) Hong Kong Government hacked by Chinese Cyberspies, FireEye says. *Bloomberg News.* Hong Kong.
VILLANUSTRE, F. (2014) Big Data Security and Privacy. *ISACA Spotlight Series India Webinar.* India, ISACA.
VMWARE (2014) World-ranked Business School rolls-out Flexible Workspaces to enhance Academic Performance. Hong Kong, City University of Hong Kong.
YADRON, D. (2016) Los Angeles Hospital paid $17,000 in Bitcoin to Ransomware Hackers. *The Guardian.* San Francisco.

Authors' Background

Dr. Gryphon Sou *earned a Bachelor of Science in Engineering Degree from California Coast University, a Master of Administration Degree from Australian Catholic University, a Doctor of Management Degree from the International Management Center – Southern Cross University, Australia and a Doctor of Education Degree from the University of Technology Sydney. He is now working as a Visiting Professor in the City University of Macau. He is also a Consultant of Hong Kong Quality Management Association and a Fellow of The Institution of Diagnostic Engineering, United Kingdom. His research interest includes quality management in big data.*