Yang Yaping

LITERATURE REVIEW OF INFORMATION SECURITY PRACTICE SURVEY REPORTS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2018

ABSTRACT

Yang, Yaping

Literature Review of Information Security Practice Survey Reports
Jyväskylä: University of Jyväskylä, 2018, 95 p
Service Innovation and Management, Master's Thesis
Supervisor: Prof. Siponen Mikko

With the development of emerging technologies, both large and small enterprises facing increased cyber security issues and challenges such as cyberattacks, cyber breaches, security workforce, cyber threats and risks and so on. The objective of this thesis is to understand the big picture of global enterprises cyber security practice by reviewing yearly information security surveys and searching for most challenging parts in cyber security management. The research is constructed based on general literature review method with the focus on providing overview of the current state of research topic and give in-depth information on the finding results. The research questions are: 1) what are the global enterprises information security practices situations from year 2008 to 2016? 2) what are the critical topics that have been addressed mostly by security professionals? 3) what are the origins, components, obstacles and improvement for critical topics?

The research reference consists of global cyber security practices surveys published by consulting companies such as E&Y, PwC, Deloitte, KPMG and security institutions such as SANS, McAfee Labs, CERT and so on. The analysis of each year topics also combined relevant academic researches and industrial studies.

The research has found nine sections that global enterprises have performed less than expected: risk management, security policy, organization of information security, human resource security, communication and operational management, access control, information security incidence management, business continuity management and compliance. These sections were extracted based on ISO/IEC 27002 standard. The finding part has analyzed origins, components, obstacles and improvement of these topics.

As for the contribution, this thesis has filled the gap between existing knowledge of organizational security practices and suggestions for further improvement. It highlights the problems in information security management during the past nine years and gives directions for organization to assess their vulnerabilities and improve practices with specific focus. Meanwhile, the extensive review also provides detailed figures in each year that can be served as reference for generating further cyber security investigation.

Key words: Information Security; Cyber Security; Computer Security, Digital Business; Information Technology; CyberAttacks and Breaches; Cyber intelligence

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The global business is expanding rapidly due to the explosion of Information and Communication Technology (ICT) innovations (Henderson & Venkatraman, 1999; Powell & Dent-Micallef, 1999; Brynjolfsson & Hitt, 2000; Melville et al, 2004; Chaffey & White, 2010; Lu & Ramanurthy, 2011). On the one hand, organizations have been largely supported and accelerated by Information Systems (IS); on the other hand, protecting sensitive information, valuable assets and intellectual property in the organizations against external and internal attacks become more sophisticated and difficult than ever before (Solms & Niekerk, 2013; Martin & Rice, 2011). As one of the important components of Information Technology (IT), information security focus on protecting information from a wide range of threats in order to ensure business continuity, minimize business risks, and maximize the return on investments as well as business opportunities.

Prior to early 21st century, the main objective of information security was to identify the potential risks and threats in critical business processes (Rok and Borka, J-Blazic, 2008), protect the financial resources (Raymond, 1990; Yang et al., 2005) as well as business reputation, and strengthen the internal compliance with regulations (Qing, Tamara, Paul and Donna, 2002; Basie, 2005). With the continuous improvement of IT and expanded globalized business, today's information security is surrounded by a variety of topics such as Internet of Things (IoT), cloud computing, social engineering, bring-your-own-device (BYOD), threats intelligence programs and so on. The increased complexity of computer science and expanded scope and scale of information security require companies to obtain a comprehensive understanding about the critical cyber security issues, problems and challenges in order to explore and mitigate their vulnerabilities and effectively protect their confidential data and valuable information assets in this digitalized world.

With the purpose of understanding changes happening in cyber security landscape and explore the impact of these changes to organizations, information security institutions and consulting companies keep examining the computer security practices in global organizations with the intent of exploring critical issues and encouraging efficient measurement, monitoring and management activities in information security. The published annual survey reports presented organizational cyber security practices situation across different industries and addressed yearly issues, problems, challenges and opportunities for further improvement.

However, since cyber threats are increasing in complexity and intensity, there is no bulletproof organization or industry when it comes to data compromise. It is worth noting, if an organization is increasing investment in detection and defense capabilities without understanding the trend of security events and the most harmful and critical security risks nearby. Meanwhile, most types of business today are the Small and Medium Enterprises (SMEs) which are known as the target of cyber criminals due to their vulnerabilities in defending cyberattacks, protecting critical information assets, acquiring technical and human resources and understanding popular security breaches than large enterprises (Yildirim et al, 2011; Ng et al, 2013; Sultan, 2010; Dojkovski, 2010). Thus, it is essential for them to put their focus on overall security health by checking the security breaches trend in recent years, assess the potential threats embedded with their business operation, IT infrastructure and industrial environment, and look for efficient and effective methods to improve their information security condition.

Based on these reasons, this thesis has been constructed with the purpose of presenting a comprehensive overview about global enterprises information security management and practices situation in recent years and searching for topics and issues that have been addressed mostly by industrial security professionals. The reviewed materials mainly consist of yearly information security survey reports that have been published by consulting companies and cyber security research institutions. The analysis of each topic also includes relevant academic researches and industrial studies.

The finding of this study presents the evolution and development of information security practices by worldwide organizations from year 2008 to 2016. The sections that haven been addressed with most frequency is analyzed in the discussion part. This enables readers to obtain in-depth knowledge about demographics of cyber breaches source as well as understand the importance of these topics for today’s digitalized enterprises. As for the industrial practitioners, the finding results can be served as primary source that facilitate the creation of current and future security crime defense strategies. Moreover, it also provides condensed knowledge for creating new information security investigations for cyber security practices.

In general, the study has been motivated by a need to obtain a holistic overview about enterprises information security practices in recent years. All the information and data that have been included and reviewed in this study can also be used by further academic researches with the similar topic of interests.

1.1 Research background

To understand the research background of this study, this part presents existing literature with similar or related research purpose. The table (table 1) below presents related researches based on category and their main findings towards organizational information security management. As we can see, main aspects such as security policy, security awareness, security standards and management have received great attention by the literature. They are certainly playing significant role in organizational information security management. To give a clear picture, the part below briefly introduces the main findings from various aspects of management. Since they are the roots of organizational cyber security management performance, the introduction will help reader to understand relevance, even the causality of research results from this study.

Security awareness which directly affects the user behavior have been addressed by literature from definition (Siponen, 2000), condition (Whitman, 2004; D'Arcy et al. 2009), measurement (Kruger, 2006), human activity (Hagen, 2008; Albrechtsen, 2010) and effect (Siponen, 2014) perspectives. Awareness generally describes the feeling and consciousness towards importance of IT security, the condition of security in organization and personal responsibilities in managing and operating information systems (Nakrem, 2007). It is the necessary condition in formulating good security culture and sufficient compliance with organizational information security policy (Kruger, 2006).

There are several conditions for achieving high-level security awareness. Firstly, awareness should be formed by motivation and attitudes, which towards security in information system (Siponen, 2000). However, this is not easy if employees do not have pre-knowledge and sense about cyber security issues. Based on this situation, the second part is to have more awareness creating activity such as group learning and peer to peer talking about security in daily work. Thirdly, evaluation and measurement of security awareness in organization is a way to check effectiveness of security awareness training program (Kruger, 2006). In the assessment, some preparation needed to complete in advance such as preparing comprehensive questions, implementing practical system for data collection, and even implementing automated tool in the measurement.

Apart from awareness, organizational factors such as budget, in-house knowledge, techniques and workforce, management-level support, security culture and security policy are also important aspects in organizational information security management.

Information security policy is the backbone of organization IT (Parker, 1998; Perry, 1985; Schweitzer, 1982; Warman, 1992). However, Siponen et al. (2002) suggested that the existing literature do not pay much attention to the policy formulation. Although IS security should always be considered at organizational level and combine with real situation, but there is a call for high-level framework. Siponen et al. (2002) has filled the gap by generating the meta-policy for emergent organizations. Existence of good policy without user compliance is not effective. According to Hagen et al. (2008), policy compliance is dependent on security awareness and training; awareness is associated with attitude and the training is the way to improve and strengthen employees' security attitude (Albrechtsen & Hovden, 2010).

In addition, compliance training plays significant role in awareness improvement. If the users do not comply with policy, then the policy and all other security solutions lose its meaning (Siponen et al, 2010). Current research has proposed some sanction-based compliance solution (Siponen et al. 2007, Straub 1990) but this theory-betrayed. The purpose of security compliance is to make employee deeply understand the policy through training and education. Therefore, Siponen et al (2010) proposed a two theories-based training program and validated it. The program was practical, and effectiveness was positive. Since the employee are the users of ISs mostly, so they have the access of critical data. By educating and motivating them to follow the policy of using ISs will significantly help the organization to avoid the internal threats (Rubenstein & Francis, 2008). Meanwhile, cultivating a good security culture has positive effect on organizational information security management since people are aware of security behavior and their own responsibilities in protecting organization critical information assets.

The other researches are more focus on risks management and security program effectiveness measurement. For the risk management, existing researches mainly focus on methodology. Since there are many security risks management guidelines exist (mainly technology-focused), Alberts and Dorofee (2002) suggested a strategy-based approach called OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). This method assumes that all security-risk-related employees participate the risk management program design and responsible for it. It generally includes three parts. The first step is to generate the threats profile based on the critical information assets. This brings an overview from organizational perspective. Employees present their ideas about critical information and discuss possible solutions for protecting these data. The second step is to detect and mark vulnerabilities in the information infrastructure. The third step is to generate the strategy and plan based on explored vulnerabilities. This approach brings a non-technical solution especially for SMEs as they can adjust it toward their own business environment. Another method called PCR (Perceived Composite Risk) was introduced by Bodin, Gordon & Loeb in 2008. This method extended the Annual lose expectancy (ALE) by bring the expected server loss and standard deviation loss in the information security investment.

As for the security program effectiveness measurement. The existing approach are performance survey (technical-measure), internal and external audit, self-checking based on standards and regulations. Besides Kankanhalli, Teo, Tan & Wei (2003), which is about developed an integrative model of IS security effectiveness, the existing literature has scientifically lacking proper and practical methodologies in this field.

Category	Article Name	Main findings related to this study
Security Awareness	Siponen (2000)	Conceptual foundation of information security awareness (nature of departure, frameworks)
	D'Arcy, Hovav & Galletta (2009)	Certain controls can serve as deterrent mechanisms for internal misuse of information
	Whitman (2004)	Information security management requires higher- level of security awareness from users
	Kruger & Kearney (2006)	Comprehensive questions should be prepared for measurement, important weighting should be obtained from relevant people, implementation of practical system for data records and automated tool should be used in measurement
	Hagen, Albrechtsen & Hovden (2008)	Awareness creating activities were less created, but awareness measurement has been commonly applied than all other measurements
	Albrechtsen & Hovden (2010)	Employee participation and knowledge creation has positive effect on information security awareness and behavior
	Siponen (2014)	Awareness training has big influence on policy compliance
Organizational factors (budgets, in-house knowledge and techniques, culture)	Qing, Paul & Donna (2006)	Two institutional forces (coercive and normative) can break the inertia which caused by low priority of security technology and internal policy to top management
	Chang & Lin (2007)	Examine the influence of organization culture on the effectiveness of implementing
	Chang & Ho (2006)	IT competence of business managers, environment uncertainty, industry type, and organization size affect ISM
	Knapp, Marshall, Rainer & Ford (2006)	Top management support enforces significantly culture and policy in organizational cyber security practice
	Kraemer, Carayon & Clem (2009)	Information security vulnerabilities are not only created by technical problem but also human factors
Security Policy (formulation, compliance,	Baskerville & Siponen (2002)	Meta-policy formulation
	Fulford &	Information security policy is fairly in

measurement)	Doherty (2003)	common nowadays, but the content and dissemination are different
	Bulgurce, Cavusoglu &Benbasat (2010)	Understanding compliance behavior from self-efficacy, attitude and normal belief
	Chang & Lin (2007)	A technical solution alone cannot keep save the organizational information security, good security strategy, adequate policy and compliance also important
	Siponen, Mahmood & Pahlina (2009)	visibility of desired practices and policy will strengthen people's compliance with information security policy
	Doherty, Anastasakis & Fulford (2009)	Security risks can be avoided by effective security policy
	Moody, Siponen & Pahnila (2018)	Organization should improve employees believe in information security policy which can prevent organization from cyber breaches. The whole organization can be at the risks if nobody aware of ISP (information security policy)
	Siponen & Livari (2006)	Six design theories for IS guidelines in exceptional situation
Security culture	Kerry, Rossouw & Lynette (2002)	Security behavior from employee accumulate the security culture ensures effectiveness of security management
	Chang & Lin (2007)	Strong oriented organizational culture has strong effect on ISM principles of confidentiality, integrity, availability and accountability
	Vroom & Solms (2004)	Security awareness should be achieved at three levels: individual, group and formal organization because they influence on each other
	Lim, Chang, Maynard & Ahmad (2009)	Organization with medium and high-risk profile should implement ISC (information security culture) to OC (organizational culture) towards better management
	Ruighaver, Maynard & Chang (2007)	Framework of eight dimensions of culture generated and explained specifically how it related to security culture

	Lacey (2010)	Analyzed why awareness campaign fail and discuss the nature of problem, solution space and practical issues and opportunities
	Tang, Li & Zhang (2016)	Information policy culture related to preserving, disseminating and managing information can help to improve information security management
Security risks management	Alberts and Dorofee (2002)	Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) approach for managing information security risk
	Warkentin &Willison (2009)	Internal risks (human fault and policy issues) how they affect security practice and how they influence interactively
	Spears & Barki (2010)	User participation brings greater awareness, better alignment between risks management and business
	Bodin, Gordon & Loeb (2008)	Using PCR (perceived composite risk) to evaluate the investment proposal in information security program
	Humphreys (2008)	An exploration of benefits, practical results and implementation method of ISO/IEC standard
Information security management (ISM) measurement	Hagen, Albrechtsen & Hovden, (2008)	Technical measures (security policy, procedure & methods) commonly implement in ISM measurement
	Kankanhalli, Teo, Tan & Wei (2003)	Developed an Integrative model of IS security effectiveness and empirically tested the model

Table 1. existing literature in information security management

Through existing literature checking, one can see clearly that there is no general review and information collection about realistic organizational information security management practice. This exposes a significant shortage of information, which should serve as the foundation of generating any organization-based security solutions and theoretical methodologies. Therefore, this study has filled the gap by reviewing recent years industrial information security performance and searching for most vulnerable parts in organizational practice. I believe this study is meaningful and necessary as the findings from can be either used as background information for optimizing current security methods and generating advanced solutions from academical or industrial fields.

1.2 Research questions and research tasks

Since the study is an extensive literature review which should starts with formulating the problem and justifying the need for review, this study is going to answer below research questions:

1) What are the global enterprises information security practices situations from year 2008 to 2016?

2) What are the critical topics that have been addressed mostly by security professionals?

3) What are the origins, components, obstacles and improvement proposal for critical topics?

To explore these questions, this study has completed the following tasks (Figure 1): Firstly, reviewing the online-accessible information security survey reports published by consulting companies and cyber security institutions during 2008 to 2016. Secondly, presenting the yearly global state of cyber security combined with most addressed topics and issues. Thirdly, categorizing these topics based on ISO/IEC 27002 standard with the purpose of identifying which part organization has encountered most problems. Finally analyzing these highlighted sections from origins, components, obstacles and improvement perspectives.

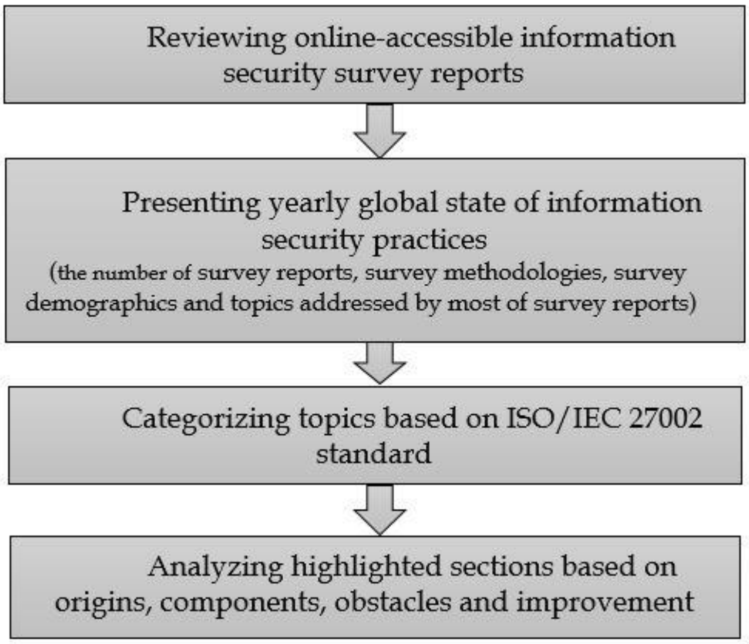
Reviewing online-accessible information security survey reports
Presenting yearly global state of information security practices
(the number of survey reports, survey methodologies, survey demographics and topics addressed by most of survey reports)
Categorizing topics based on ISO/IEC 27002 standard
Analyzing highlighted sections based on origins, components, obstacles and improvement

Figure 1. Research tasks

The process of completing these research tasks is presented as follows: the preliminary step is to choose the population of studies (Cooper, 1982) which is a group of potential survey reports to be reviewed in this research. According to Mathieu and Guy (2015), researcher must identify a range of information sources to ensure that "reviewers accumulate a relatively complete census of relevant literature". The second phase is to screen and assess the quality of resources to determine whether the information provided is useful in regards of completing the review purpose. Most of survey reports that have been selected to review are either focused on annual global state of information security or regional state of cyber security are industrial-focused, and all the survey responses are collected from investigated companies across different sectors; Therefore, these trackable and reliable empirical statistics bring high quality of review resources to this research. The third step is to select and extract data that includes the most relevant and useful information that pertain the research objectives. Since there are several most-emphasized topics that have been extracted based on the review of security practices reports in each year, thus, all the selected information and data are retrieved based on these topics and used for explaining those. Finally, the researcher needs to organize, categorize and summarize the evidence "extracted from the primary study" to make a new suggestion or contributions to the current knowledge (Jesson et al. 2011).

1.3 Structure of thesis

The thesis is divided into six chapters. The first chapter introduces the subject of study and research background. It also presents the motivation and purpose of conducting this research as to fill the gap in existing studies that have explored the state of enterprises information security practices in recent years is somewhat in short supply. Meanwhile, the first chapter also states the outcome of this study and describes the importance and necessity of this work.

The second chapter describes the literature review methodology and data analysis methods. It also states the way of finding and selecting literature review resources and retrieving the most relevant data towards the selected topics by security practice survey reports in different years.

The third chapter constitutes the main part of this research which is the review of enterprises cyber security practices based on a reversed timeline, from 2016 back to 2008. This chronological review presents the development and changes happened during this period and clearly reveals the most critical and challenging problems in enterprises information systems security management and improvement.

The finding chapter categorizes the critical topics based on ISO/IEC 27002 standard in order to show the most criticized part by security reports and provide a relatively quick benchmark for relevant studies by industrial practitioners and researchers.

The discussion part analyzes each section from perspectives such as origins, components, development trend and solutions.

The last chapter concludes this research, discusses the credibility and reliability as well as suggests the possible direction for other similar topics of interests.

1.4 Definition of key concepts in information security

Information Security Management

According to Eloff and Solms (2000), the aim of information security is to protect the information systems and establish a framework by which organization can run information systems operation as they are expected. Information security management focuses in minimizing the risks of information systems in the operation. There are number of steps included: first, a planning phase allows company to set up security objectives, identify the assets to be protected and choose the framework for implementation; second, implementation phase allows the plan to be implemented. During this step, risk assessment and mitigation, training employees about security issues as well as assessment and audit are constantly conducted. Finally, security management should be an ongoing procedure. Managers, IT functions and employees should be constantly aware of security issues and maintain this process to achieve a long-term benefit.

Principle of information security – C-I-A traid

There are three characteristics that constitute the principle of information security: confidentiality, identity and availability; which are commonly called C-I-A traid. These three characteristics are not necessarily connected or dependent on each other, however, if there is problem occurring in any part of this traid, the others are consequentially affected. Confidentiality guarantees that only authorized parties or processes with sufficient privileges could access to the information. Integrity ensures that information is only created, modified or deleted by authorized parties. Availability ensures that the information can be accessed in a timely and reliable way when people or applications need it. These three characteristics can also be goals or objectives of information security since they together represent three very desirable properties of information system.

However, Anderson (2003) points out that the C-I-A triad is just the beginning of information security. To extend the principles, he suggests some additional properties such as authenticity, accountability, non-repudiation and reliability. He provides a new definition of enterprise information security which is also called “A well-informed sense of assurance that information risks and controls are in balance”. This definition fills the gap which ignored by other definitions and shed light on the importance of governance and management for achieving the security of ISs.

Cyber threats and cyberattacks or breaches

Cyber threats are defined as the potential risks towards information, life, operations and properties. They are brought by the adversaries or people who exhibit the strategic behavior to exploit the cyber space with the purpose of gaining benefits (Anderson et al., 2012). Cyberattack refers to the sabotage created through using ICT towards confidentiality, integrity and availability of information systems or the residence of information systems.

Information security policy

Information security policy is a well-written and clearly defined strategy towards protecting information systems security and maintaining secure practices to the resources and network of organization (SANS, security policy, 2007). A general content of information security policy includes password policy, risk assessment, user responsibilities, policies of using Internet, policies of using e-mails, disaster recovery and incidence detection (SANS, security policy, 2007).

Information security governance

Cyber security governance refers to a set of responsibilities that are assigned to those people who are responsible for governing and managing security practices for protecting the information systems security in the organization (MITRE, cyber security governance, 2010).

ISO/IEC 27002

ISO/IEC 27002 is an information security standard which has the objective to "provide management direction and support for information security in accordance with business requirements and relevant laws and regulations" (ISO/IEC 27002). It outlines fifteen sections that need to be addressed when implementing security controls and security practice activities. A brief content of each section can be found in finding part according to the official standard.

2 RESEARCH METHODOLOGY

2.1 Literature review

Literature review is generally a review of all the existing literatures that related to a specific topic. It can be either a background study for an empirical research or a standalone piece of work that provides valuable contribution in the specific field (Jesson, Matheson & Lacey, 2011). As to the background study, the review provides "understandings of the topic, and what has already been done on it, how it has been researched, and what the key issues are" (Hart, 1991). Moreover, a background research can also help the researcher justify the needs for research and select the appropriate methods to conduct the research (Levy & Ellis, 2006).

As for standalone literature review, it provides an "overview and analysis of the current state of research on a topic" (Harvey, 2010). The objective of standalone literature review varies in different research, for example, evaluating and comparing previous research on a topic and provides in-depth information about what is known to "reveal controversies, weaknesses, and gaps in current work" (Harvey, 2010), or synthesize the existing literature to a mature level, or facilitates the theory development work" (Webster & Watson, 2002). Cooper (1988) concluded taxonomy of literature reviews in which he categorized the types of review based on characteristics of focus, goal, perspective, coverage, organization and audience (Table 2).

Characteristic	Categories
Focus	Research outcomes; Research methods; Theories; Practices or applications
Goal	Integration: generalization; conflict resolution; linguistic bridge-building Criticism; Identification of central issues
Perspective	Neutral representation; Espousal of position
Coverage	Exhaustive; Exhaustive with selective citation; Representative; Central or pivotal
Organization	Historical; Conceptual; Methodological
Audience	Specialized scholars; General scholars; Practitioners or policy makers; General public

Table 2. Taxonomy of Literature Review by Cooper (1988)

According to Mathieu & Guy (2015), a high-quality standalone literature review provides trustworthy information and insights knowledge of the past research and enables the other researchers seek new direction on similar topics of interest. Besides, the outcome of this research can also be used as the references in the similar field or as a resource for other studies.

Since this thesis is conducted with purpose of obtaining a holistic overview of global state of enterprises cyber security practices in recent years and concluding what topics have been investigated and discussed mostly by security specialists and IT professionals, it can be considered as a standalone literature review with the focus on "research outcomes" and goal of "identifying central issues". In addition, due to shortage of studies with the same purpose, this study also presents an important role in both academic and industrial field.

Although literature review can be conducted with different purpose and methodologies, the general process of conducting a literature review is somewhat in common. The following part briefly introduces the general procedure for conducting a literature review.

The first step is to formulate the research problem which the literature review is going to answer. A research problem is significant for guiding the entire study because it provides the direction of where to collect the resources, and how to select the relevant data that is useful for the research. The second step is to explore and select the review resources which is potential to be used for the research. Researcher at this time should identify quantifiable amount of review sources for screening and evaluating the quality and applicability for further analysis. The third step is to screen for inclusion and exclusion. A set of rules and selection criteria needs to be established for determining the relevance of resources (Mathieu & Guy, 2015). After this, researcher should gather the applicable information concerning to the research topics from each primary study (Cooper, 1982). Okoli and Schabram (2010) emphasize that gathered information should be mainly based on the research question. Meanwhile, researcher should also pay attention to the methodology that the primary study has implemented, as well as research design and methodology. Finally, with retrieved data researcher must categorize, analyze and summarize the evidences in a way that the research suggests a new contribution to the existing knowledge of the topic.

Generally, literature review should present the researcher's knowledge about a specific field and demonstrate the researcher's own interpretation concerning the research topic through answering the research questions. Besides, reliability and validity should also be emphasized through demonstrating the reliable and trusted resources that included in the review. Researcher should also criticize the purpose, scope, authority, audience and format of the literature review (Brown, 2006).

2.2 Research Strategy

This sub-chapter presents the research strategy that consists of data collection, data screening, data quality assessing and data extraction method. Based on the objective of this study which is to conclude the global state of enterprise information security practice in recent years (2008-2016) and summarize the most emphasized topics by industrial security professionals, the data in this literature review mainly consists of enterprises information security practices and data breaches survey reports published by consulting companies such as E&Y, PwC, Deloitte, KPMG and computer science and security institutions such as Computer Security Institute (CSI), SANS, McAfee Labs, Computer Emergency Response Team (CERT). Meanwhile, data analysis part also includes relevant academic and industrial studies with the similar topic of interest for richening the information about the critical topics from diversified perspectives.

The overall process starts by searching the relevant online-accessible cyber security survey reports. Since most of these resources are not academic but industrial studies, Google search engine has been mainly used for collecting the primary data. To avoid being overwhelmed by the volumes of data and obtain accurate knowledge, keywords such as "computer security", "information security" and "cyber security", and key words combination such as "computer security survey", "information security survey report" "cyber security review" have been used to limit the retrieval results. The data collection process has ended when a point of saturation has reached, which is 2008 due to less available relevant survey reports. However, it is likely that new articles focus on 2017 enterprises information security management will come after the data collection phase in this study, but the analysis has only made based on current online accessible resources in order to achieve the scope by focusing on current state of affairs.

The second step is to cull the most relevant and potentially useful information from the collected articles and reports. Since this study is mainly focused on analyzing the topics that have been widely addressed by global cyber security surveys, reports that made with specific focus such as regional or industrial cyber security situation are less relevant. However, they remain the role in supporting topic analysis. The irrelevant data that are excluded from the processes are reports that were generated by students for degree thesis, small-scale research and pure technical report. The reason for excluding these is because they do not have strong validity to support the analysis within the global context. They are either narrow-scoped or small scale to represents the global enterprise population.

In the data evaluation phase, data has been extracted and evaluated based on the scope of the study. The coding method has been used to record the extracted data based on several criteria: name of report, issued year, key findings of survey, focus of report and discussion about topics among years. According to Borg, Gall and Borg (1996), a coding method can facilitate the process by generating a narrative summary about the knowledge related to the research questions. The process should be iterative and develop until the level of information saturation has been achieved.

The goal of this process is to identify the information that serves as the input data for the analysis process and provide evidence for the integrated and synthesized review results. Meanwhile, by using the spreadsheet it is easy to find the most relevant information to the research questions and observe the summary of each year studies combined with key issues that have been discussed by different reports in specific years. The following part presents review of each year cyber security situation.

3 OVERVIEW OF INFORMATION SECURITY SURVEY REPORTS RESULTS

3.1 State-of-affairs of 2016 information security surveys

From the time of data collection, there are 24 online-accessible information security reports in 2016. Among those, 11 reports focus on global state of cyber security, 4 reports explored the security breaches and risks in United States during 2016, 2 reports examined United Kingdom state of cyber security and the rest were focus on the topics such as cloud security, BYOD and mobile security, state of endpoint security, CIO survey and so on.

The number of participants in global survey is ranging from 234 to 10,000. Most of respondents are from North America, Europe, Asian pacific and South America. Nearly all the participants in the global survey are board level executives (CEOs, CIOs, CFOs, CISOs) and other IT and security professionals. Most of companies in the investigations are large and medium size enterprises with more than 2,000 employees and mainly operating in key segments such as finance, energy, business services, government, retail and healthcare.

Because of the enhanced understanding of organizational information security issues, improved cyber security awareness and developed enterprises information security structure, 2016 global cyber security reports present an encouraging atmosphere. SANS report about IT security spending trend reveals that information security budget is increased in main industries such as financial services, technology, government, education and healthcare. PwC 2016 global state of information security survey report also presents that the average information security spending rose 14% in this year. Besides, new emerging technologies such as mobile data, cloud storage and big data are driving the changes in accessing and organizing information. These technologies certainly help the companies to avoid the damage from attack and its significant impact. More than 60% of respondents in PwC survey run their IT function in the cloud and use managed security services for company's data security. More than 50% of them employed the biometrics for authentication and big data for cyber security management. Although companies benefit from advanced techniques, the potential risks brought by using high-techs also make them feel vulnerable and weak regarding risk exposure. Indeed, there are still many things for business to do to "adequately protect themselves" and fully incorporate the benefits brought by technologies into data security management (Dell, 2016).

However, increased security budget and improved security management did not significantly slowdown the growing number of cyber breaches. Symantec report reveals that by the end of 2015, there was 318 data breaches occurred during the year, 429 million identities exposed with average 1.3 million identities exposed per breach (Symantec, 2016). According to IBM and Ponemon institute "2016 cost of data breach survey", the average costs of each data breach are for example 355 dollars in healthcare industry, 246 dollars in education, 221 dollars in financial, 208 dollars in services. Clearly, cyber breaches are going to cause unprecedented damage to todays' organizations. There are still existing a big gap between security investment and effective protection solution for the sensitive data. It is not enough to just build the firewall against the attack since everyone can be victim of the cyber criminals and provide outsiders access to the company's internal information. A comprehensive and strategic framework is required to strengthen the overall fundamental system.

Based on the review of existing 2016 cyber security survey reports, the following topics have been seriously addressed:

- Security as an enabler and protector of business
- Cyber threat intelligence for anticipating cyber risks
- Continuous training and education helps to implement new techniques for protecting sensitive data

According to PwC's survey, many information and business executives nowadays understand the information security as a business enabler and protector instead of inhibitor or hindrance. For many years people understood cyber security as costs from IT or unnecessary part since it cannot either against the information threats or directly solve the business problem and boost the growth. However, the expanded scope of business and the digitalized world make more and more business practitioners realize the advantages and opportunities of information security. For example, today many products have integrated the embedded value which offer the after-sale or customized services for consumers through Internet. This requires company to proactively thinking cyber security and privacy issues in order to deliver high quality customer experiences and build the brand trust. However, although cyber security has moved beyond cost to enabler, privacy and data security in external environment are still among the top security concerns when using new technologies to maximize business benefits. For example, IoT brings the significant challenges in protecting PII (personal identification information). Big data expose the sensitive information to everyone. According to Dell's report, 90% of respondents in their investigation have big concerns about the data they have uploaded to the clouds. In the working place, microchips and sensors implemented makes employee feel worried about their privacy. When the fear pervades along with the security concerns, it is difficult to estimate whether new technologies indeed bring advantages to business more than disadvantages.

Meanwhile, with the emerging of interconnected virtualized corporation, different businesses are leveraging this global information infrastructure to serve customers as "one company" and thus formulate the "network economy". This requires a well-organized information exchange system to enable secured information collection and utilization by different stakeholders, business entities, customers and suppliers (Deloitte & Touche, 2003). There are many security challenges in establishing this global coordinative infrastructure. For example, the legacy system and different interfaces may result in difficulties in consistent authentication; different regulations and legal requirements applied to different information platform can also result in challenges in data protection by information transformation. Understanding and structuring solutions to these challenges require company to have clearly assigned accountabilities to the people who access to the information. Besides, it also requires the system designer to integrate the specific mechanism in order to detect the important node or critical pathway for malicious attempts (Donnet, Gueye & Kaafar, 2010).

Generally, business operators should understand the whole picture and find the solutions that integrate the information security in all the functionalities, not only the major processes. Meanwhile, non-stop learning for new trend in cyber security helps business to proactively protect themselves in the further development.

The second addressed topic is about using cyber threat intelligence to anticipate the potential risks. With the growing number of cyber threats and cyber breaches, the analysis, discussion and self-learning around those cases are developing and organizing a database for anticipating more advanced and sophisticated cyberattacks. In essence, threat intelligence helps company to proactively understand the strategy of cybercriminals and establish the plan for potential risks that may exist in the future. Through the review, there are several notable changes happened in 2016 and these highlights the importance of establishing the CTI by organizations to fight back with defensive strategy.

According to "IBM X-Force Threat intelligence 2017", 2016 is notable with some "record-breaking metrics such as the number of previously leaked records that surfaced during the year and an increase in the size and scope of DDoS (denial-of-service attack) attacks" (Figure 2).

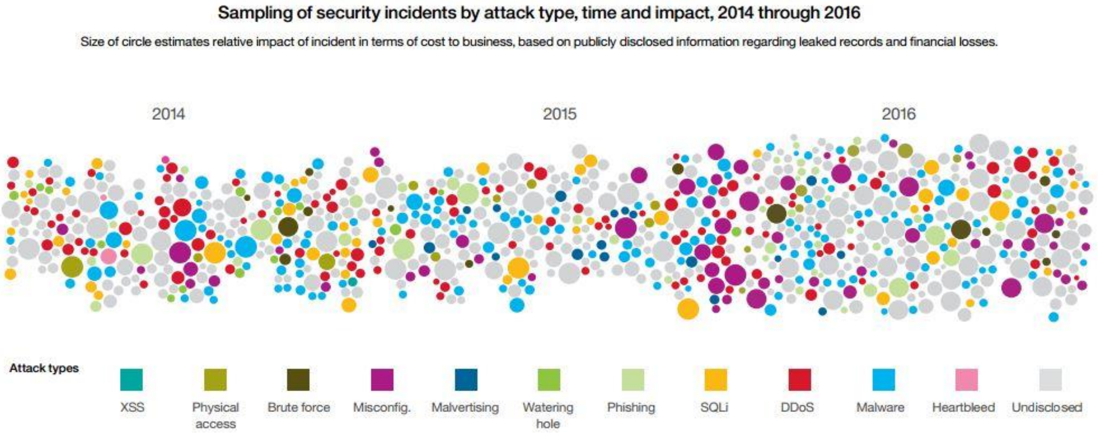

Figure 2. Sample of security attacks based on type, size, time and impact from 2014 to 2016

Obviously, 2016 has more than double amount of the leaked records than previous years combination. Among those security misconfiguration, malware and DDos have increased in both size and impact. The results of those are visible in physical world, for example in 2015 winter, hundreds of thousands of people in Ukraine have suffered the outage of electricity due to the malware attack. Besides, the largest information leak, "Panama Paper" has hit thousands of prominent people in commercial and political circles. To minimize the risks of being attack, government and organizations must identify their positions in the cyber environment and employ the defensive strategies in overall processes.

The other notable changes in 2016 compared to previous years is that data breaches have shifted its focus from structured data to unstructured data (IBM X-Force, 2016). For example, in previous years data breaches were often related to password, credit card number, ID or personal health information (IBM X-Force, 2016). However, in 2016, data that were exposed to outside were content of emails, critical document were related to government or law, industrial financial information and so on. For instance, 1.4 GB information about people interests were leaked through Qatar national bank in 2016. In the same year, Philippines voter registration system has been hacked and it resulted exposure of 300 GB voters' information such as fingerprints and passport information. The shift on the structure of data reveals that the value of data becomes more and more important and beneficial for cyber criminals who owns different purpose. SANS reports (2016) point out that organizations should not only analyze their past artifacts in order to secure the business, but also understand the relevant information related to their business in terms of risks and value.

Because of the high volume of cyber breaches and unusual situation compares to previous years, it is essential for decision makers to reevaluate their investment in information protection and think beyond the scope of their business information security. Taking advantage of up-to-date threat intelligence can tremendously help organizations to improve its capabilities against cyberattacks while strengthen its overall functionalities by nonstop learning and developing the security knowledge in worldwide context.

The following part briefly discussed about how to use CTI in estimating future trends in complex cyber security landscape combined with typical case happened in 2016. Generally, there are two different types of data resource for establishing organizational CTI: External and Internal (SANS, 2016). Internal source is basically built up from organization own cyber security assets, while external data source consists of open-source (public blogs, tweets, feeds), closed-source (underground information) and networking source (governmental and industrial sharing). As for the internal source, organization may leverage the past cyber breaches to which it has encountered, to train their employees cyber security awareness. Organization may also study the explored vulnerabilities and related indicators from same industry and relevant segment. To achieve this, organization can create a threat profile as a checklist to avoid potential risks which come from inside and proactively manage the incidence which come from outside. As for the external resources, today organizations may purchase commercial source of threat intelligence to strengthen their capabilities with up-to-date information and early-discovered indicators. According to EY report (2016) about how industrial practitioners look at the cyber intelligence program, nearly 40% of them says that it is unlikely to detect sophisticated attacks by themselves. However, on the other hand these companies don't have CTI program implemented in their IT infrastructure. This may explain the reason of high volume of vulnerabilities, which IBM X-force report has found in 2016. Meanwhile, in EY report (2016), only 10% of the companies described that they have constructed their TI program by collecting internal and external resources to analyze the relevant information in industrial cyber security environment. One of the industrial accidence can approve this result. It is known that spam email is listed among top toolkits for hackers to steal company's internal information. Malicious malware attached with email also provides cyber criminals chance to unlock the encrypted information. In December 2016, an electricity transmission substation has de-energized for several hours, which has resulted one fifth of Kiev out of electricity. This was then analyzed as the attack by an industrial malware called "Industroyer", which was invented with the purpose of destroying Industrial Control System (ICS). Clearly, companies without CTI implemented will not receive early warnings from external resources and thus, decisions-makers will not place the security operations in advance to against cyberattacks.

Another important finding from threat intelligence report in 2016 is that top industry such as financial, government, information and communication, healthcare and manufacturing are the top targets in cyberattacks. As an example, information and communication industry often suffered by stuck buffer overrun (IBM X-Force, 2016). This is related to the weakness of programs which provides possibility for overwrite the memory and give controls to the hackers. In Financial industry, thousands of companies and banks were suffered by cyberattacks to their messaging system that were designed for customer to transfer the money around the world. Millions of US dollars were stolen or illegally transferred to criminals account by this SQLi attack which is a code injection technique for exploring the vulnerability of system (SQL Injection, Wikipedia). Obviously, CTI program is a survival toolkit for companies to gain expertise, methodologies and techniques in data and technology protection. It provides companies a proactive method to analyze cyber security issues and internal vulnerabilities, especially when CTI has combined with overall business infrastructure. A powerful CTI not only deliver the insights of previous tailored cases but also give a clear picture for decision-makers to invest in data security operations.

The last topic that has been seriously addressed in 2016 reports is continuous training and education for improving both security awareness and knowledge of employees in implementing new techniques in their working life. Although the quantity of cyber breaches continued growing in 2016, the support from executive level concerning enforcing the security policy, strengthening the education and training of cyber security awareness and investing more budget on constructing security infrastructure enables organizations becoming stronger in the cyberattacks. According to ISACA and RSA global report (2016), nearly half of the directors were concerned about organizational cyber security issues. Among those 63% are CIOs who oversees cyber security in the organization. As to the executive support to the mitigation of cyber security risk, 66% of executives enforced the security policy followed by 63% in providing appropriate budgets and 58% in developing the security awareness training program. While the security topic is getting more and more important in organizational practices, still there remains problem of finding suitable professionals who has advanced skills and knowledge in handling and managing sophisticated security issues. The report reveals that more than half of the respondents do not believe their employee can handle anything else than simple cyber security incidence. In 2015 (ISC)^2 report about global security workforce study, the shortage of advanced security professional is widening. 62% of survey respondent states that they have few experts working in their organization compares to 56% in 2013 ((ISC)^2, 2015). This indicates that the reason for hindrance of improving security performance is rather limited skilled resources than investment and other subjects.

As mentioned previously, malware is among top cyber incidence sources in 2016. Phishing emails, as a delivery method of malware remains popularity. Email continues to be the primary communication method for most organizations nowadays. Phishing emails, messages or website links are designed for stealing information when victims click the link or reply the email. In general, most of phishing emails include grammar mistakes, spelling mistakes, trustable party from no matter internal or external, and threats or rewards such as the victim's account will be permanently closed, or victim got reward from some campaigns. If the employee has no ability to recognize the phishing emails, he or she will provide the access to cyber criminals for company's information such as customer information, financial information, intellectual properties, corporate management resources and so on. According to Telstra survey in 2016, one third of business in Asia and Australia has suffered the malware attack by phishing emails and the impact has last over a month. APWG report about phishing activity trend in 3rd quarter of 2016 also present that China (47.23%), Taiwan (43.88%), Turkey (39.01%), Russia (37.86%) and Ecuador (37.21%) are the top countries of phishing infection, while Scandinavian country such as Sweden (20.33%), Finland (19.81%) and Norway (19.73%) has the lowest infection rate.

In general, organization should constantly train their employees about cyber security breaches and suspicious manner resulting the internal information leakage. Organization which has no plan for investing security training should use other initiatives to control the privacy such as access control for the suppliers, security audit for internal and external security vulnerabilities, cyber security insurance, cyber security intelligence, application testing. Meanwhile, for internal IT staff, enterprise should not rely upon "on-the-job training", however, an intensive and skill-based training should be conducted constantly, and the training result should combine with the performance analysis (ISACA, 2016). Besides, the skill-based training should also focus on new techniques being employed by company.

3.2 State-of-affairs of 2015 information security surveys

There are 62 cyber security reports found in 2015. Among those, 15 reports focus on global information security situation, 4 reports focus on healthcare industry security practices, 11 reports focus on regional cyber security situation (United States, United kingdom, East Asian countries, Australia and European countries) and the rest were written with specific focuses such as cyber security in boardroom (Veracode, 2015), Security Awareness Survey (SANS, 2015), the State of Mobile Security Maturity (ISMG & IBM, 2015), Critical Infrastructure Readiness Report (Aspen Institute, 2015) and Intel Security (2015) (Figure 3).

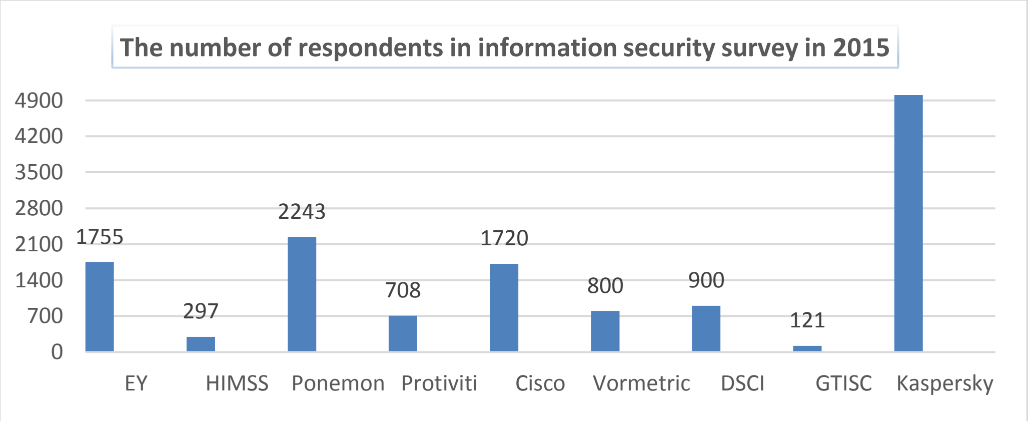

Figure 3. The number of respondents in information security survey in 2015

As to the population of global survey, around 600 information security directors, board executives and IT professionals from different types of businesses across major industries (Finance, IT, Government, Industrial Manufacturing, Telecommunication, Energy and Retail trade) have participated the surveys. E&Y, Kaspersky, PwC and Ponemon institution have investigated over 1000 participants globally. Others have included around 200 to over 10,000 people locally or regionally as sample population (Figure 4).

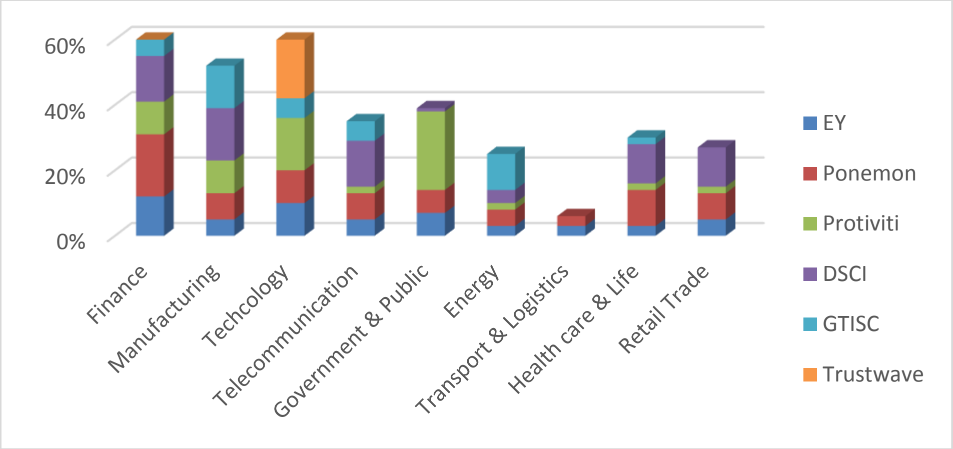

Figure 4. Respondents by industry sectors

In 2015, cyber security is more sophisticated than ever due to digitalized business and more advanced and complicated information technology. The attacks which were previously mainly targeted on public sectors, broader organizations with valuable assets and financial services, have extended to individual and small corporation level (TiEcon, 2015). Cyber criminals have used advanced tools to get inside the organization’s networks even faster than most businesses can react against. On the other hand, small businesses which often think they are too small to draw attention from cyber criminals are under cyberattacks due to consistent vulnerabilities and immature information security program. With the growing number of cybercrimes and development of security intelligence, more and more corporations realize that they need to strengthen overall cyber security infrastructure to improve ability in protecting sensitive information and reacting to incidence in a short time (SANS, 2015).

According to E&Y (2015), only 36% of respondents at the anticipation stage state that they are unable to detect the sophisticated threats compares to 56% in the previous year. Meanwhile, only 34% of companies feel vulnerable compares to 52% in 2014. This is a notable improvement in terms of practices and awareness of cyber security in organizations. However, companies still need to design and implement cyber threat intelligence strategy and encompass the security together with organizational business in order to understand its position in cyber security war and get ahead of security crimes.

Because of the landscape of cyber security has changed and expanded along with the digitalization, the main focuses of 2015 information security survey are:

- Inside threats

- Internet of Things (IoT)
- Threats intelligence and
- Constrains of information security improvement

The following parts will explain each topic specifically by presenting the statistics from 2015 combined with big cases happened in 2015.

The first addressed topic is about inside threats. According to Louis J. Freeh who is the former FBI director in congressional testimony, "perhaps the most imminent threats today come from insider". The insider may use his or her access to harm organizational security through unauthorized disclosure, data modification, espionage or other related actions which will result the loss or damage of the company's resources, capabilities, business operation and customer loyalty. Statistics from E&Y global survey in 2015 shows that more than half of survey participants think employees are the most likely source of cyberattack compares to 36% who think external cyber criminals as the likely source. Meanwhile, Insider Threat Spotlight Report in 2015 presented by Linkedin also shows that 62% of security professionals think inside threats have become more serious and frequent in last 12 months and they are more difficult to detect and prevent than the outside attacks. Obviously, internal threats are far more harmful than external threats because they are associated with different reasons such as organizational control and monitoring, human behavior, financial incentives from outside criminal groups, business competitions, personal hobby and so on. One of the data breaches happened in 2015 can explain the danger of insider attack. A former employee and contracted chiropractor of Wisconsin-based Harel Chiropractic & Massage accessed and removed roughly 3,000 chiropractic patience from clinic. That information includes name, addresses, phone number, email number, social security number, birthday and so on (scmedia.com, 2015). Another case from 2014 is the employee who worked as internal audit in financial department in British Supermarket Morrison, has stolen and leaked over 100,000 payroll databases to outside journalist due to the company has found that he use a mailroom to sell market products on ebay (ITproportal.com). This cyber breach resulted the company to spend more than 2 million to fix their database. Nevertheless, spotting the insider attack is more difficult and tricky since perpetrator can have authorized access to the internal sensitive information. However, there are numerous ways to avoid the harm of insider threats such as access control, profile-screening before hiring the employee, continuous training, education and audit. Besides, companies should establish a comprehensive security strategy and constantly measure and monitor their practices in order to prevent data exfiltration at the early stage.

With the development and widely adoption of digital devices used at workplace, it is urgent for organizations to know their internal and external security environment. They must identify the critical assets to their business, check employees' background before signing them responsibility to handle sensitive data and draw a picture of "what would hurt the most" when cyber events happen. Luckily, we can see some positive situation in this counterattack. Inside Threats Report presents that 75% of executives from information security function are constantly monitoring security configuration and controls of the applications. More than half of the respondents in E&Y report define the data leakage and data loss prevention as the highest priority tasks in the upcoming months. Meanwhile, Governance of Cyber security 2015 report published by Georgia Tech Information Security Center present that there is a significant increase from 17% to 79% in cross-organizational committee during 2008 to 2015, which implies that organizations have realized the benefits of cross-organizational collaboration in identifying and addressing inside threats, combating external cyberattacks and improving the governance effectiveness.

Indeed, human factors are the critical part of internal threats. No matter what techniques implemented to prevent data loss, organization should never stop "incorporate inside threat awareness into periodic security training for all employees" and develop the inside threat program in order to proactively identify and mitigate the threats before it become mature (Common Sense Guide to Mitigating Insider Threats 4th Edition, CERT program).

The next topic is about IoT. With the further development of Internet and digitalized services and devices, IoT is getting more and more popular in different industries and businesses. It is more than catchphrase but a serious issue to be discussed today.

While the digital world evolving, information network comprises of mobile devices, telecommunications, sensors and physical objects, have extended to a wider range. On the one hand, IoT accelerated the connection of devices and enabled convenient access of information. On the other hand, unsecured objects have been growing more and more with a greater exposure of risk and potential to be attacked. According to a CTIA (the Wireless Association) white paper about mobile cyber security and IoT, by the end of this decade, there will be 50 billion devices connect with IoT, which means that around six devices per person on the planet connecting to IoT. A recent study by HP found alarming statistics in the IoT space: 70% of tested devices contain security exposure, 90% of devices can be used to extract at least one piece of personal information, nearly 80% of devices did not require strong password which has sufficient complexity and length and 70% of devices allows attackers to identify valid account through account enumeration. With massive security issues coming along with IoT, companies are urged to reconsider this rapier in digitalized world and seek for advanced security strategy to face the challenges brought by IoT.

According to PwC global cyber security survey report, "the number of respondents who reported exploits of operational, embedded and consumer systems increased 152% over the year before". One third of survey's populations have security problems relate to IoT. However, only 42% of organizations in E&Y's survey have the department which focuses on impact of emerging technologies on company's information security. 68% of survey respondents do not realize that monitoring business ecosystem in IoT is a critical information security challenge. It is obvious that companies have not yet prepared for this explosion of devices and information. The rapid development and change on cyber security requires digitalized business to formulate an in-depth defense and protection approach against known and unknown attack, data loss and leakage, information compromise, unauthorized access and other information security threats (Cyber security and the Internet of Things by E&Y, 2015).

According to PwC's report, some organizations start to realize the importance of defining the common privacy and information security rules when cooperating with other players in IoT world. Since the embedded systems are most vulnerable to be exploited by cyber criminals in IoT, by doing so companies can ensure the stakeholders of IoT adhere to information security standards and protect the customer private information by deploying new techniques and security protocols in this ecosystem. However, it is difficult to reach balance between value of those systems and information security concerns. Businesses that are striving for the success in digitalized information society should be partnering with other players to sharpen their security intelligences and against the outside threats together. E&Y's report point out that there should be a trusted security network between manufactures and consumers in which both side can search for the value and achieve the win-win situation.

Another emphasized topic among 2015 cyber security surveys is the cyber threat intelligence. According to a SANS survey "Who is Using Cyber Threats Intelligence and How?", threat intelligence refers to "the set of data collected, assessed and applied regarding security threats, threats actors, exploits, malware, vulnerabilities and compromise indicators".

There are sufficient information security challenges faced by today's organizations. For example, large scale organization investment (e.g. without good prioritization filter, many security alarms and operational chaos enough expertise, one-fit-all solution and inadequate security tools rely) on past events or signature. Although companies strive to be successful in managing different innovations and controlling cyberthreats from inside to outside, continuously increased cyber breaches their counter strategy. The essence behind threat intelligence is to enable business to "recognize and act upon indicators of attack" before it creates huge impact to the organizations (SANS, 2014).

According to E&Y 2014 global cyber security survey report, only 36% of respondents do not have cyber threats intelligence program in their organizations. Half of the PwC survey respondents have invested in core safeguards for example active monitoring and analysis of security intelligence to better defend the evolving threats in ecosystem. 47% of survey respondents have leveraged the cloud services for strengthening company's cyber threats intelligence. These statistics shows that companies have demonstrated an increased focus on cyber threat intelligence. Based on SANS (2015) cyber intelligence survey report, there is a notable improvement of company's capability of incidence response. For example, 51% of companies see more accurate and faster response to the cyberattacks. Besides, 48% noticed the incidence deduction due to early prevention by CTI. In addition, more than 50% have implemented CTI to some extent. However, the evolving threat landscape also highlights the trend of threats brought by emerging technologies which most of companies have not yet prepared against. As mentioned previously, IoT was one of the main themes in

2015 cyber security landscape. The features of IoT being seriously concerned are: firstly, IoT devices are everywhere, they are not only home devices but also wearable and portable devices; secondly, all IoT devices are embedded with mobile or cloud technology; thirdly, interaction of devices performs a key feature of IoT. Thus, communications between those interacted devices can be misused by cyber criminals (ENISA, 2015). CTI program should provide critical gateway which can detect malicious IPs and website and secure the network devices.

E&Y (2015) emphasize that companies can explore the potential damage of cyber threats and understand the value of identified potential risks by their security operation center (SOC) and cyber threat intelligence program. The deeper understanding of survival environment, the easier they can prioritize their spending and avoid the waste investment in control techniques and equipment (E&Y, 2015).

Ponenmon 2015 global cyber security megatrends report reveals that most of countries involved in the survey believe their cyber security posture will be improved for specific reasons such as implementation of CTI and advanced data protection techniques, sufficient support from board level executives and valuable resources from cross-organizational collaboration. More than half of the survey respondents think cyber intelligence activities are the critical part for protecting information assets. 47% will strive for the improvement in cyber threats intelligence in the next three years. Nevertheless, creating the professional cyber intelligence requires capabilities to transfer the raw data and unfiltered feed into processed and sorted information. Such information should also be accurate, complete and actionable for employees to use. In addition, it is important for companies to understand the context which refers to the motivation of attack in order to effectively prevent similar situation in the future (SANS, 2014).

The next topic is about several constrains for improving information security management. According to E&Y 2015 global report, there is no significant improvement from 2014 to 2015 in companies' information security practices. Only 12% of respondents think their security function fully meets the organization's needs. 67% are still in the progress of improvement. Meanwhile, 47% do not have SOC, compared to 42% in the previous year. One third of participants think they should invest to their security function up to 50% in order to support the business development. Although there is no need to discuss about strengthening information in today's companies, there are still many constrains that affect the improvement progress. For example, insufficient human and technical resources, less-structured plan and cyber threat intelligence, employee-related issues and limited investment for information security solutions (Ponemon, 2015). The following part analyzes some of the constrains and highlights obstacles in current cyber security practices.

The first constrain is information security investment. It is known that an effective investment can significantly reduce the cyber threats and support the need from business functions. Meanwhile, it also helps to maintain the compliance and ensure the cultural fit in the organizations since constant security training and education can improve employees' awareness and train their secure behavior (Xiuyan Shao, 2015). Besides, investment for security policy development can help organizations to establish effective governance structure and define specific policy for internal and external environment. In general, the purpose of information security investment is to generate a return which can be tangible or intangible benefit (Tsiakis and Stephanides, 2005).

Since strong leadership is the critical part in building successful security program, a sufficient investment is an essential requirement for achieving this objective. Moreover, as mentioned above, cyber threats intelligence, risk management practices and incidence response management are the critical parts for protecting organization against internal and external attack, information security investment should spare no effort to ensure that these functions have been created and constantly developed.

Based on statistics in E&Y 2015 global security survey, 84% of respondents will spend the same or less investment on information security for IP in the upcoming year. 70% will spend same or less amount investment on security operations such as antivirus, patching, encryption and so on. 62% will have same or less amount of budget for improving organization's incidence response management capabilities over the coming year. Indeed, less investment brings less return benefits especially in performance improvement and security awareness (Pauline & Elizabeth & Joan, 2007). However, most of organizations have not realized that their investment in cyber security is just in the beginning phase. The evolving digital world requires responsive investment in new security approaches and techniques to defend the versatile attacks (E&Y, 2015).

Luckily, we can see some positive situation in some industries such as financial, health care and retail trade with together 93% of organizations identified their need to protect data and willing to increase the protection budgets during the coming year (Vormetric Inside Threat Report, 2015). Meanwhile, it has been observed that many companies have leveraged the big data to address the security issues. Around 40% of companies in Ponemon's study state that their company is investing in big data analytics for cyber defense. Besides, 59% in PwC's report are implementing the big data analytics for security (PwC, 2015). Nearly 60% of security professionals in SANS's report said that their big data play important role in detection and response efforts. Cyber threat intelligence will combine with these naturally when analyze market matures (SANS, 2014). Indeed, a digitalized organization without a well-defined cyber security investment plan can easily fall behind the trend and lose its initiative to control the security situation. The dependency of organizational assets and operations on information and technology requires companies to recognize information "as a strategic enabler" and set up a strong governance and financial support for protecting information security in daily business operations.

Another constrain for improving companies' information security performance is employee-related risks. Inside Report (Linkedin, 2015) reveals that 46% of investigated security professionals think their regular employees pose biggest insider threats to organizations. United State National Cyber Security Examination Sweep Summary found that 25% of broke dealers noticed that their employees did not follow the firms' identity authentication procedure have resulted loss from fraudulent emails. Meanwhile, 55% of respondents in Vormetric insight threat report said that privileged users have posed the largest risk to organization, with 35% think ordinary employees are the main type of privileged users. Since the inside threat have become more difficult to deal with, organizations should seek for "well-meaning" employees and strengthen the inside access controls to prevent the internal data breaches (Vormetric, 2015).

Today, all types of information business and even government have possibility to be the target of cybercrimes. Symantec 2015 Internet Security Threat Report point out that there has been a steady increase in cyberattacks targeting SMEs in 2015, which proves that all sizes of organizations are under attacks. Although "no business is without risk", human factor is always the weakest part in security reviews (Symantec, 2015). Therefore, Symantec report suggests that "every employee should be part of the effort to stay digitally healthy". Besides, boardroom should understand what risks they face and proactively manage the situation through CTI and other data analytics methods in order to build a wall for customer data and customer loyalty before cyber criminal's attack (Symantec, 2015).

Concerning the human factor, many reviews also mentioned about insufficient skilled resources such as IT staff who has the skills to investigate the internal threats. They are constantly being demanded by market. According to (ISC)2 2015 Global Information Security Workforce Study, 62% companies were lacking cyber security professionals compared to 56% in 2013. 57% in E&Y survey and 47% in Ponemon's study also admit that there haven't been ample resources to ensure security function to meet business requirements and contribute value to organization. With increased number of sophisticated cyber threats and extensively developed new technologies, skilled security professionals are highly demanded due to high priority of information security among organizational decisions.

Whether investment in personnel or technologies, organization need to observe the changes in internal and external environment and highlight the critical part of data security that will eventually affect the business needs (E&Y, 2015). On the other hand, most of cyber breaches today are well-planned and made by resourced cyber espionage group which may have a wide variety of purpose as well as resources to conduct the simultaneous attacks (Symantec, 2015). This raise the question how companies can arm themselves against those intelligent groups since today few organizations have sufficient in-house resources to secure their information assets. E&Y report suggests that conducting an effective objective assessment helps organization to understand its security exposure. Organization should assess the maturity of security functions and map the road for the future investment that can sustainably support the business strategy. Meanwhile, the assessment should always be listed in the boardroom memo so that everyone is informed of direction and way to reach the target.

3.3 State-of-affairs of 2014 information security surveys

There are around 26 security surveys reports found in 2014. Among those, 12 reports focus on global cyber security situation, 2 reports focus on health information privacy and security issues, 9 reports have summarized the regional security practices situation such as Japan, United States, Australia, United Kingdom and North American countries. Other reports were written with specific focuses in information security, for example the governance in today's IT security department (Ponemon, 2014), insights about password security, cloud security (Lieberman software, 2014), and cyber security audit process and capabilities (Protivit, 2014).

Besides large consulting companies such as E&Y (n=1825) and PwC (n=9700), most of organizations have examined around 500 enterprises in their security practices survey across different industries. Figure 5 present companies and institutions which have included the population size of their information security survey. Finance (include insurance and real estate), technology, manufacturing and telecommunication are the top industrial sectors in the investigation since they are most prone to cyberattacks. Meanwhile, some surveys have also included governance and public sectors in the investigations since breaching government and national information can bring huge benefits for cyberattackers nowadays.

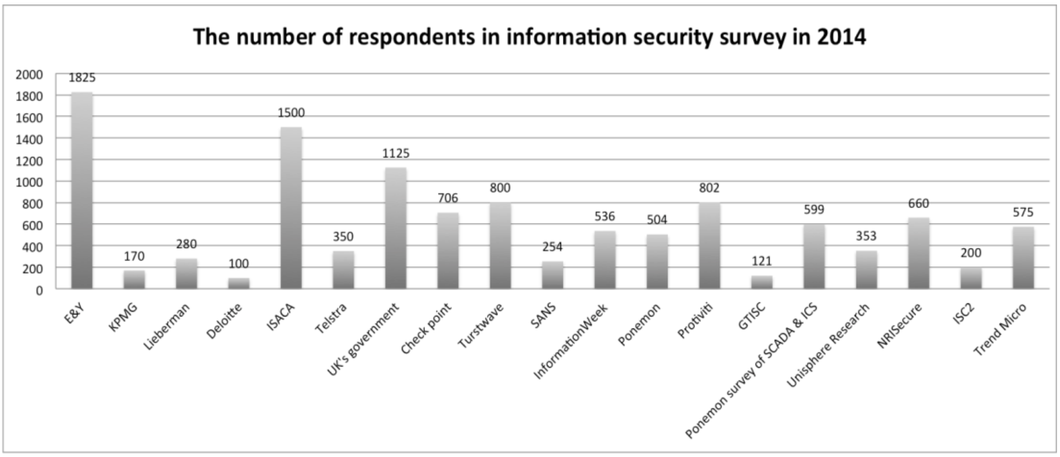

Figure 5. Population size in information security survey in 2014

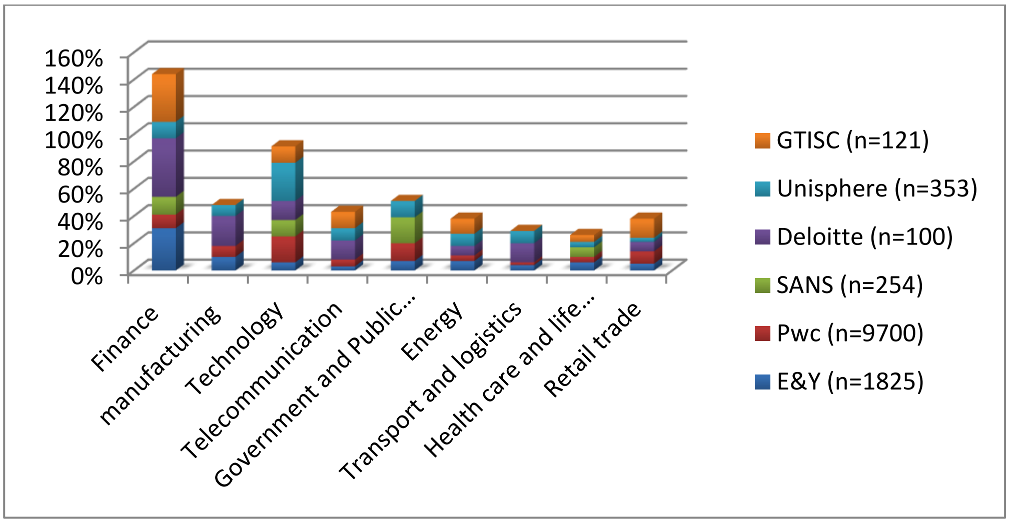

Figure 6. Respondents by industry sectors

Most participants in 2014 global cyber security surveys are SMEs in which most of respondents came from board level executives such as CIO, CISO, IT executives and other decision makers. This has ensured the quality of survey results since they are familiar with their own IT infrastructure and organizational cyber security practices situation (Ponemon study about SCADA and ICS, 2014). More than half of the respondents came from EMEIA (Europe, Middle East, India & Africa) areas and Americans, the rest were from Asia-Pacific countries.

According to Finra's (Financial Industry Regulatory Authority) report on cyber security practices in February 2015, the most significant cyber threats that majority of companies considered in 2014 were: cyber risk of penetrating system with the purpose of stealing financial information and data, operational risks associated with physical environment and natural disaster, and insider threats. E&Y's report (2014) also presented the similar results. Security threat that have increased the organization's risk exposure in 2014 are: cyberattacks with target of financial information and intellectual property (more than 25% of respondents rated as top priority), disruption of organization's business and reputation (25% of respondents rated as top priority), internal attacks by disgruntled employees and natural disasters (15% of respondents rated as top priority).

Not only are the threats growing, also company's vulnerabilities and the most vulnerable resources in cyber defense have been considered by nearly all the survey reports. Ponemon's study on cyber security in critical infrastructure points out that database, applications, mobile devices and desktops possess high-level vulnerability in the network area. Around 40% of respondents stated that use of insecure network, cloud services and social network brings more possibilities for cybercrimes. Given the fact that security risks cannot be eliminated if companies rely on digital devices and information systems in business management. They must have a comprehensive understanding of cyber threats, incidences and breaches in order to estimate the security climate change and improve their security management efficiently (PwC, 2014).

Based on review of 2014 information security reports, the most cited and investigated topics are:

- Risk management
- Technical controls
- Cyber security governance
- Incidence response management
- Human resource security management
- Cyber security insurance

The following part analyzes each topic by combining 2014 statistics and big events happened in the same year.

The first topic is about risk management and this has been addressed by nearly all the survey reports. It is known that today's information security risks associate with human errors, internal and external threats, advanced digital technologies, company's security infrastructure and management. How to identify, assess and treat risks in accordance with organizational overall security infrastructure becomes a difficulty for most of digital organizations. According to SANS "An Introduction to Information Security Risk Management" (2006), the purpose of risk management is to "understand and response to the factors that may lead to failure in the confidentiality, integrity and availability (C-I-A triad) of an information system". In general, company should ask questions such as: What risks associate with our information systems? How these risks will affect to our business? How to assess and manage these risks? What kind of techniques and tools we can use to manage risks successfully? By answering these questions organization can understand uncertainties and potential threats in their business management and thus effectively improve their security strategy.

Finra's observation on firm practices in 2014 shows that nearly 90% of firms have established information security risk assessment programs. Among those, some firms have used one or more of the NIST, ISO 27001/27002 or ISACA framework. Others have implemented part of these standards in various functions of their assessment program. The report also found that firms have adapted a variety of risk assessment and management approaches in their security activities. For example, some have devoted more resources on protecting critical assets and information, some have conducted the risk assessment annually and generated the yearly summary and report. Trustwave (2014) suggests that regular security risk assessment and penetration testing are critical since they can help the business to understand the location of their critical assets and information and whether those are vulnerable under an attack. Unisphere (2014) emphasizes about the data professional expertise on understanding information security risks and how they ultimately affect business. Generally, since the ever-changing landscape of cyber security and IT bring difficulties in estimating and managing uncertainties, companies should consistently maintain comprehensive risk assessment in order to analyze and estimate the potential of danger and select the suitable tools and approaches to reduce the harm at maximum level.

Another cited topic by 2014 cyber security survey reports is the technical control, which refers to using technology to control the access and usage of critical and sensitive information in order to minimize the damage by cyberattacks. Generally, it includes data encryption, identity and access management (IAM) and penetration testing (Finra, 2014). Encryption ensures that only approved users can access the data. It provides an effective countermeasure for companies to against data leakage and exposure (Finra, 2014). IAM facilitates the management of access of information resources through "enabling the right individuals to access the right resources at right time for right reasons" (Gartner website). Penetration testing focuses on exploring the weaknesses and vulnerabilities of the information systems by simulated attack.

According to PwC's report in 2014, only 59% of respondents have secure access control measures; 55% of respondents have encryption of e-mail messages, intrusion detection and prevention tools, and unauthorized use or access monitoring tools. Since the most vulnerable network areas to cyberattack are applications, database, mobile devices while the least are access control system and authentication system (Ponemon, 2014), it is significant to build and strengthen the technology control in order to protect the critical information that transferred between those systems and against the unauthorized access, modification and disclosure. Meanwhile, some reports emphasized the technology control especially when partnering with the third parties and acquiring new information systems from them. Trustwave's report mention that company should only cooperate with those third-party system providers who have "detailed and lock-down policies, perform ongoing and regular penetration testing", as well as "demonstrate the remote access controls". This can ensure not only the maintenance of those systems but also the isolation of company's private information from other customers. One of the best practices is the Lockheed Martin. This is an American global aerospace, defense, security and advanced technologies company and it provides all military products and services to their clients such as military and intelligence department of local government (Wikipedia.com). They have very pro-active assessment of all their suppliers' security readiness. For example, they require their suppliers with whom they provide sensitive data to fill the cyber security questionnaire for better understand their capabilities of managing sensitive data and cyber security readiness (ISACA, 2014). As cyber security capabilities evolve, suppliers should constantly update the questionnaire. Moreover, they organize the collaboration session for suppliers to discuss the newest cyber threats and best security practice in order to bringing the gap between company internal and external resources for better risk management.

According to ISACA's report, even though technology controls can prevent or delay the cyberattacks to some extent, constant educating and training people, as well as improving their knowledge and awareness of cyberattacks should not be ignored.

Cyber security governance is a common addressed topic in all the years. According to "Information Security Governance: guidelines for boards of directors and executive management" by IT Governance Institute (2010), a well-established information security governance can reduce the uncertainties in the business operation and support the efficient risk management and information security decision making process. A governance structure that has clearly defined roles and responsibilities of the individuals and information security objectives can provide guidelines for security practices and address security issues in all the levels inside the company (Finra, 2014). GTISC (Georgia Tech Information Security Center) report with the focus on information security governance emphasizes that how boards assign and organize the committee responsibilities will largely affect the security management effectiveness. Their data shows that around half of the investigated companies have separated audit committee and risk committee, which is a big improvement compared to former years: 8% in 2008, 14% in 2010 and 48% in 2012. PwC report shows that around 45% of respondents have their board executives involved in overall security strategy. Deloitte reports shows that nearly 60% of respondents believe senior management commitment can largely improve the organization information security levels. Meanwhile, they also suggest that effective information security governance should include both preventive and detective strategy so that company can avoid unwanted event from unauthorized access and identify the occurrence of unwanted event efficiently.

In today's advanced technology world, security executives and board of directors should not only be in charge of business management but also risk management and information security governance in order to make wise decision to achieve the overall business objectives (PwC, 2016).

Another topic that has been addressed seriously in 2014 is the incidence response management. No matter the extent of defense, it is evitable that incidence will occur at some point. Therefore, incidence management and response are very important capabilities for companies to decrease the impact of incidence and prevent it happen again in the future.

Generally, it includes four critical steps: preparation, detection and analysis, containment and recovery, and post-incidence activity (Higher Education Information Security Council, 2014). On the preparation step, company should gather resources for handling incidence as much as possible and develop a communication platform for incidence response once it happens. On the detection and analysis phase, company should train and educate employees different types of incidences and how to detect and analyze them in order to avoid those in the daily work. Meanwhile, people also need to understand how to report or escalate the incidence and use proper tools and methods to decrease the impact at the maximum level. On the post-incidence level, company should learn from the breaches, understand the weakness in their information security practices, and seek for improvement. For example, create the incidence portfolio and measure the effectiveness of policy and strategy.

However, through the review, companies are often failed in this critical part. Only 20% of respondents in Delotte's survey have developed incidence response plan. 33% of respondents in EY's survey prepare to invest more resources to strengthen their incidence response capacities. Less than 20% of respondents have real time insights on cyber risks. About 14% of respondents in PwC report have the plan to invest more in incidence management response process in the next 12 months. Besides, Finra report also found that firms have inadequate response to cyberattacks due to insufficient data protection, user's awareness training and supervision of the outsourcing management. Obviously, the number of cyber incidences is growing rapidly in digital world, "ranging from passive monitoring to close-in attack" (Deloitte, 2014). Organizations are suggested to establish the security operation centre (SOC) to analyse the known cases and constantly monitor the incidence response plan and procedure in order to strengthen the response capabilities and decrease the amount of loss to the minimum level (E&Y, 2014). The best practice of incidence response perhaps come from national government, since they organize the prevention and response to cyberattacks and establish contract between public and private sector in order to prescreen the incidence before it is public to outside. It facilitates the communication of detected vulnerabilities and stimulate the vigilance (ISACA, 2014).

The next topic is about human resource management which in most of cases refers to employees' training and education on security issues. According to ISACA report, although technical and administrative controls can support the prevention and detection of cyberattacks, insecure human behavior still remain weakest part in information security management. Training staff about their secure behavior of using information systems and proper reaction when encountering potential threats are significant for achieving good security results.

PwC report point out that "employees are the most-cited culprits of incidence". Their data about source of incidence in 2013 and 2014 shows that the severity of inside threats is much higher than external threats. US state cybercrime survey also presents that nearly one-third of respondents in their report admitted that inside crimes are more harmful than outside incidences. Besides, ISACA report found that nearly 80% of companies have given mobile devices to their employees, while 90% of them have experienced the big loss of mobile devices assets in 2014. This implies that employees are unaware of protecting company's information assets, as well as unaware of damage from cyberattacks to their company.

With development of advanced mobile technology, many companies are choosing flexible way of working such as BYOD (bring-your-own-device) and online working. However, this also create opportunity for cyber criminals to steal company's information and exploit the critical resources. For example, malicious application, which usually cannot be removed fundamentally, can steal information saved in the phone. In addition, loss of computer devices can create internal information leak if the employee was using own devices in the work. Thus, organizations should clearly defined information security policy in the trend of BYOD and social engineering in order to limit potential risks that come from inside. Meanwhile, prescreening employees' profile before hiring them is another way to ensure the quality of human resources. In general, organization should constantly measure their information security practices from employees to alter the awareness of cyber security issues and potential risks in daily working life (E&Y, 2014).

The final topic in 2014 global cyber security survey is cyber insurance. During the couple of years, cyber breaches and attacks have become more common and the impact of them ranging from national level to individuals. A data breach not only can create huge lost but also influence business reputation, customer trust and even the whole business lifecycle (Lawrence et al, 2003). Purchasing a cyber insurance is an effective way to recover from the damage. Besides this, many cyber insurances also include notification to customer about cyber breach, restoring customer data, recovering compromised data and repairing damaged systems (Baer & Parkinson, 2007).

Through the review, there are lot of active purchases of cyber insurance. GTISC report reveals that 48% of the respondents were reviewing their cyber insurance for cyber-related risks in 2015, compared to 28% in 2012 and 27% in 2010. 61% of companies in Finra's review have purchased the standalone cyber insurance. PwC report also states that respondents from South America lead the purchase of cyber insurance, with 58% stated that they have purchased the policies. This implies that companies understood this as a necessary cost for strengthening overall cyber security system. However, according to Reuter.com, an article called "Insurers struggle to get grip on burgeoning cyber risk market" reveals that insurance company feel hard to find suitable person to handle the case since they are often requiring rigorous security evaluations. So, many companies are paying more than they received. Those people who handle the product often just conduct a limited questionnaire with questions like do you have cyber security procedure in placed instead of a detailed assessment and audit of overall process. This may affect the inappropriate evaluation of the risks price and results in less attention to some potential threats that lie in the current business model.

No matter the size of business, security breaches are inevitable for all the companies in the information world. Organizations which have strong security intelligence program and well-established security operation systems are certainly stronger than small business who has fewer resources in security war. Therefore, it is more important for SMEs to consider purchase cyber insurance to have more control over their cyber security situation.

3.4 State-of-affairs of 2013 information security surveys

There are 21 online-accessible information security surveys found in 2013. Among those, 10 reports focus on global cyber security situation, 4 reports focus on United States cyber practices, 2 reports have examined cyber security practices in United Kingdom and the rest were focusing on Australia, Ireland, Netherlands and Latin American countries.

Besides large organizations such as PwC (N=9300) and (ISC)2 (N=12,000), most of surveys have investigated around 400 companies across different industries, only five surveys have included more than 1000 respondents. Respondents came from finance, manufacturing, technology, government, public sectors and energy industries (Figure 7). Meanwhile, several surveys have also included respondents from professionals and personal services industries. This is due to the labor market of IT professionals and information security professionals has expanded because of highly demand of advanced knowledge and skills in information security field (ISC2, 2013).

According to PwC report, cyber security crimes have become more advanced and sophisticated during 2010 to 2013. On the one hand, information companies have acquired more comprehensive and deep understanding of cyber security issues; on the other hand, cyber criminals are developing their expertise and investing resources to improve their skills in exploitation and attack. IC3 (the Internet Crime Compliant Center) report presented that there are 262,813 complaints reported in total in 2013, with 119,457 reports concerning a loss. The total loss reported are 781,841,611 dollars. Although there is no clear scope of cybercrime, IC3 point out that cyber criminals are using different ways to scam and defraud Internet users.

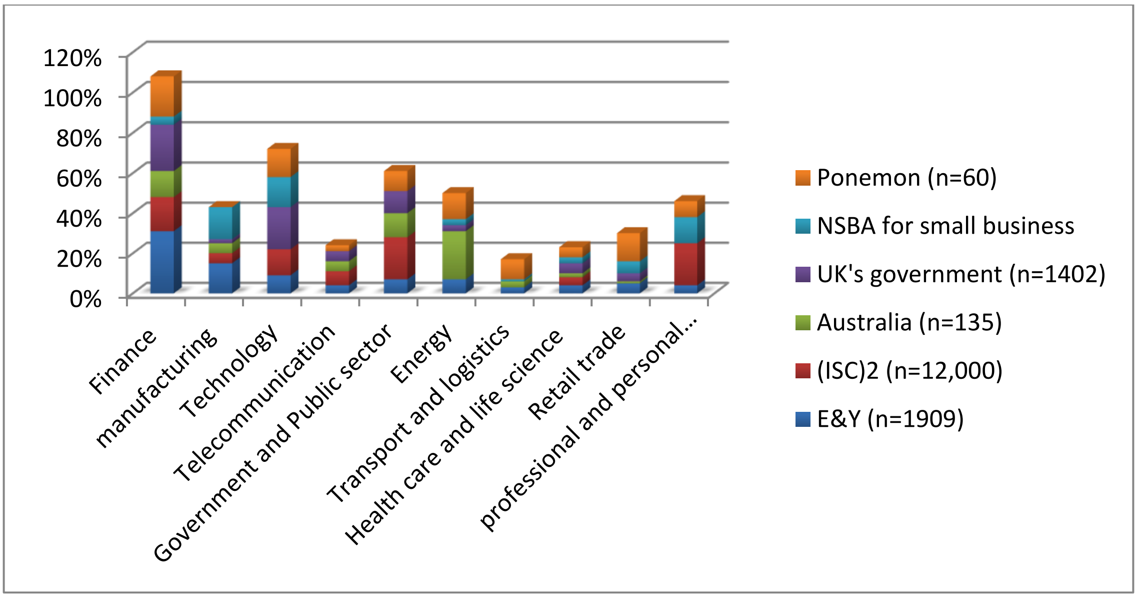

Figure 7. Main industries of respondents in 2013 global cyber security survey

2013 was the year of mega breaches based on Symantec report. The total number of breaches in 2013 is 62% greater than 2012 (253) and 2011 (208). Eight breaches have resulted more than 10 million identities exposure compared to one breach in 2012 which resulted same amount of exposure. Some famous cases happened were: malware installed in Target Point-of-sales which affected 40 million payment cards. Hacked Adobe system provided access to encrypted credit card information of millions of customers and compromised the account information of millions more (Securityweek, 2013).

Among those, zero attack vulnerabilities bring more chances for hackers to exploit the system. Symantec data shows that the amount of identified zero-day vulnerabilities is double than 2012 and more than the total amount of two previous years. Meanwhile, social media scams and malware are flourishing on the mobile devices. Norton report reveals that about 38% of mobile devices users had experienced mobile cybercrimes in 2013. Although stolen and loss of devices remain the biggest problems, insecure behavior of using mobile devices are considerably affecting the data security and open the door to cyber criminals (Symantec, 2013). Based on these situations, the critical security concerns in 2013 lie on below topics:

- Administrative and technical control of information security
- Security audit and control
- Incidence response plan
- Board involvement
- Technical skills of employees
- Information security awareness training

As mentioned in 2014's chapter, security control not only can help companies to identify its own vulnerabilities but also govern the implementation of organizational security policies in daily business operation and strengthen the overall system through a series of laws, regulations, guidelines and techniques. As for the administrative controls, Symantec report suggests that company should define BYOD policy and make sure that it is in place to ensure that employees-owned devices are under control when access Internet and expose to the network. Besides, company should also enforce an effective password policy in which rules of creating password has clearly defined. For instance, the password should contain at least 8 characters, 2 digits and special characters. This will significantly help the company to strengthen the access and avoid security breaches.

To avoid the zero-day vulnerabilities, companies should update their systems, applications and programs regularly, especially when the vendor has released the patches. SANS critical control, which is one of the security control framework, also emphasizes the importance of continuous and proactive assessment as well as remediation of system vulnerabilities in order to find the "hole" and fix it before exploited by attackers. While technical controls can be implemented in many ways from firewalls, anti-virus software to advanced techniques to limit the Internet access and also defend the malware and spam. Generally, company should establish security control based on its security objectives and scope. Meanwhile, they should regularly assess the vulnerabilities of their operating systems in order to get ahead of the crimes.

IT security audit refers to "the examination of the practices, procedure, technical controls, personnel, and other resources that are leveraged to manage companies' security risks and assures that they adhere to recognized best practices and IT security mandates" (Tracysecurity.com). Statistics from AICPA (American Institute of CPAs) report shows that about 87% of cyber incidence can be avoided if company conduct information security audit. Meanwhile, UK security breaches survey sponsored by PwC also point out that large corporations are more diligent to check the security information when partnering with third party vendors. For instance, they obtained more times audit rights than small businesses, which enabled them to evaluate the adequacy of security of their business partners. Besides, HIMSS (Healthcare Information and Management Systems Society) security survey also found that healthcare organizations are likely to conduct audit to their IT security plan in order to proactively measure the information security situation that might cause huge damage to both customers and healthcare organizations. In addition, CSI (Computer Security Institute) has also ranked the cyber security audit as the top weapon in cybercrimes prevention and detection. AICPA report suggest that an effective audit plan will significantly help the company to identify the potential security risks and consequently avoid or decrease the damage from inside. In addition, EY report concerning internal audit plan in 2013 also addressed this important self-optimization a way to better combat with increased risks from both outside and inside. In general, company should proactively and constantly conduct security audit, and those major risks that were identified by the audit must be analyzed and sorted into CTI checklist (AICPA, 2013).

The next addressed topic is incidence response plan and management. As mentioned above, incidence response consists of several steps with the purpose of protecting company's critical information, information systems and computer assets when encountering to the computer incidence (Wikipedia, Computer Security Incidence Management). Whenever cyber incidences happen, the security team or IT staff should handle this event based on a clearly defined incidence response plan (Computer Security Incidence Management, Wikipedia). The plan should include the instructions to response to security incidence meanwhile minimize the damage from breaches (TechTarget. com).

According to Bit9 report, nearly half of their survey respondents have experienced the cyberattack during 2013, among those 33% prioritized the business disruption or employee downtime as the biggest impact that came along with the cyber incidence. E&Y report also shows that nearly 31% of their survey respondents noticed the increase of security incidences during last 12 months. 59% of respondents cited the increase of external threats to their company. However, only 5% of respondents in E&Y examination have confidence on their computer incidence response capabilities and important security approaches such as threats intelligence program, data protection program and vulnerability identification capability. UK government has issued "The Ten Step" in 2012 for guiding the business to protect themselves in cyber security, however, the results from practices shows that incidence management step received less attention by SMEs.

Obviously, this important tool for remediation and correction has not received enough attention by companies based on the survey results. Since the number of security incidences is increasing, organization that has not yet established the response management are more vulnerable when cybercrimes occurred. Thus, AICPA report suggests that it would be good to start the prevention from security controls, which has been defined by security professionals as the best practices to guide the company to identify its vulnerabilities and forecast the potential breaches. Meanwhile, E&Y report also emphases that organization should invest less in maintenance but improvement and innovation for self-optimization.

The following part discuss about board involvement in cyber security practices. PwC report found that most of investigated companies still lack sufficient support from board level executives. Their statistics shows more than half of the respondents think the top-level is the biggest obstacle in improving information security effectiveness. Meanwhile, insufficient expenditure, in-house technical skills, poorly integrated information systems are the other major obstacles in building efficient organizational security program.

Why board level engagement is important for security practices? There are few reasons behind. Firstly, cyber incidence can affect the overall business chains, not only in single department or division. A cyber breach can leak company's critical information such as customer data, financial information and other sensitive information that may put the entire enterprises in a difficult situation. So, the decisions which are related to attack response must be instituted by higher level executives. Secondly, with understanding of organizational cyber security readiness, it is much easier for board level to comprehend their business from a worldwide perspective. They are in the perfect position to know how the competitors manage the security issues and where the enterprise is today, and where it is tomorrow. Thirdly, mobile and cloud technology is evolving, and information organization must identify the appropriate ones and implement those into business process. Board level should always keep in mind the risks and benefits from advanced techniques so that they can select the good choices for company and avoid the risky options. Finally, the best security practice is always achieved by security culture, especially the orientation from boardroom. Just like the punishment for Sisyphus in Greek mythology, the entire organization must put the rolling ball back forever unless it gets support from highest level. Nevertheless, worries for large scale business often come from business operations, credits or customer perspectives, cyberattacks are growing rapidly and developing toward all types of business. Board level executives should also put cyber security issues into their list and prepare for the upcoming incidence.

Since most of reports show that the readiness security program is not yet ready, higher level executives in those organizations should also be accountable for achieving objectives of their security program. They must lead the team to develop the policy and prioritize the assets to be secured from the attacks. Otherwise, security will rather narrow down to the compliance checking, and pass the test result to the regulators than block and response to the attack successfully. Besides, executives need to support the information security function by defining the company's security appetite, measuring the performance, aligning the business strategy to information security strategy and integrating information security decision into organizational decision-making process (E&Y, 2013). Since cyber security affect all the parts of business, board level executives must have adequate knowledge and in-depth understanding of security goals in order to make wise decisions.

The next found addressed topic is workforce with technical skills and comprehensive understanding of information security. Obviously, this crew can help the company to survive in the cyber security battle. According to a study made by Frost and Sullivan business consulting, "Demand for security professionals in the Americas is increasing by 12% annually, with 164,000 jobs forecast in the next year alone" (2012 ISC2 Global Information Security Workforce Study) (Figure 8).

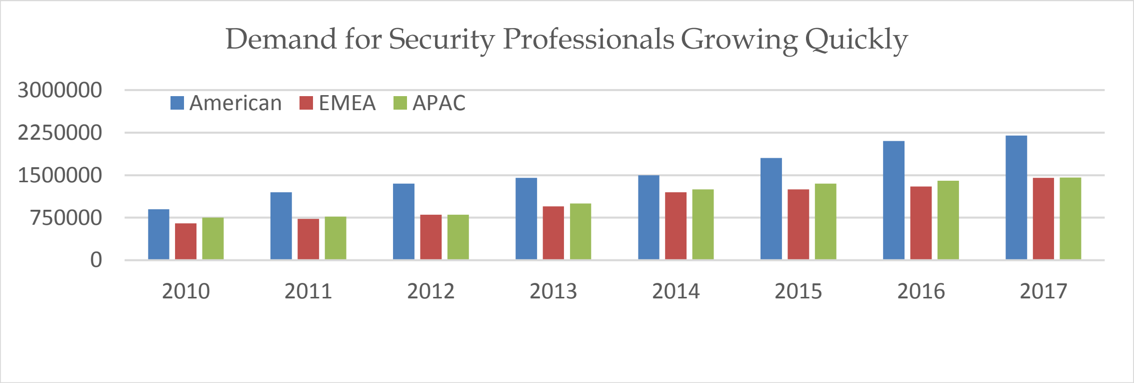

Figure 8. Demand of cyber security professionals growing rapidly

From the table we can see that the market demand of security professional is increasing not only in US but in all the regions. However, practically if the company's core business is not security, it is difficult to make any huge investment decision on searching security professionals. Yet, TechTarget.com also mention that it is difficult for company to find the person who knows how to drive the plane rather than explain to them how the plane flies. Statistics from PwC's report reveal that one of the biggest obstacles for company to build effective security function is the absence and shortage of in-house security professionals. Although colleges and universities are training and educating people who are qualified to the entry-level position in security industry, IT security professionals may end up being too senior for most enter-level positions (TechTarget.com) while fresh graduate don't equip with sufficient knowledge and hands-on experience to take equivalent security jobs.

Considering the obstacles in finding suitable human resources, below part generally introduces a framework based on "Practical guide to manage cyber security workforce" published by Council on Cybersecurity in 2014. It gives guidelines for companies to manage cyber security workforce while integrate with company's investment strategy and cyber security goals.

The guideline starts by analyzing the workforce management lifecycle. All types of business should consider their critical information assets protection strategy no matter they are small business or global corporations and government institutions. The best practice should include three important factors: People, Technology and Policy. The stating point can be everywhere depending on which step company has performed already (Figure 9).

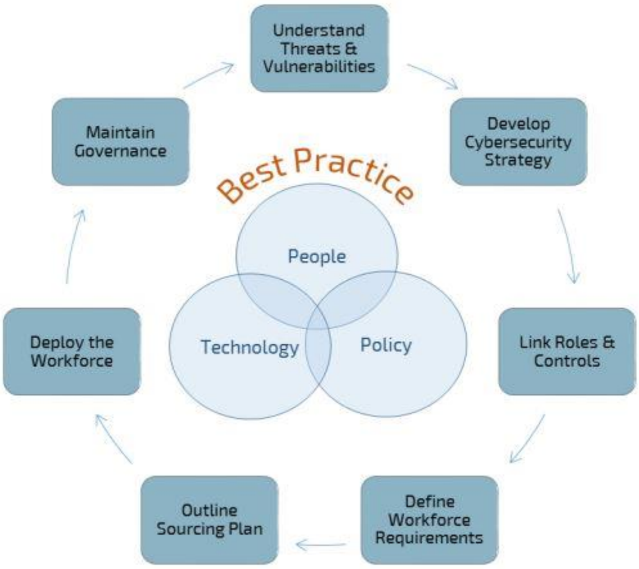

Figure 9. Cyber security workforce lifecycle

Understanding risks and vulnerabilities is the first step when entering the management lifecycle. Statistics shows that corporation leader often understand the big trend in cyber security landscape, but they are unaware of specific threats and risks which are targeting to their business or industry. By analyzing the vulnerabilities executives can obtain greater awareness of cyber security issues and define security objectives based on current profile. This step does not require big investment since there are many available tools for basic vulnerability assessment such as comprehensive questionnaire, internal audit and third-party solutions. The second step is to develop a security strategy combined with enterprise business strategy and cyber security objectives. Company should involve all important stakeholders and senior level executives to committee to discuss the practical plan and responsibilities for each party. A common understanding of overall situation and target should be achieved at this stage. The next process is to link the roles to units and personnel. A checklist of existing roles for handling cyber security tasks is vital to explore the needed positions, which gives the direction for the next step. After this, organizations should be very clear about what kind of security workforce they need and what requirements should these people have in order to fulfill the gap and facilitate security practices. When deploying the workforce, company should not only consider the responsibilities but also the cost and reporting structure within the chain since this person will be powerful in defending breaches and protecting sensitive information. Meanwhile, a prescreening of employee's profile can largely affect the deployment success since internal threats remains biggest problem in all the years. Once in place, corporation should constantly manage and strengthen the governance of security practice, capture the feedback from frontlines and update security strategy regularly for achieve better performance. The execution of these steps requires time and resources but helps the organization to prioritize the tasks.

The next topic addressed in 2013 is insufficient security awareness training and education. It is known that security awareness training should be conducted into entire HR process, from pre-employment, during employment to the termination. Consistent training helps employees to refresh their knowledge on cyber security issues and strengthen their awareness of responsibilities in daily operation. However, many surveys found that companies do not seriously address this topic. E&Y global survey report has used one chapter to present cyber security training situation among investigated organizations and provides suggestions for improvement. From their statistics, only 6% survey respondents have very matured security awareness, training and communication. Around half of respondents have developed the training program and one third of survey participants have not yet developed or even planed it. PwC (2013) report also shows that nearly half of respondents do not have employee security training in their companies. This may explain why the security response plans are not effective and why the most significant security threats come from inside of the organization (PwC's report). On the other hand, people tend to forget to do tasks that are only done rarely. So, security awareness training which requires expensive workforce may add obstacle to the progress. It is also difficult to find appropriate person who could conduct the employee security awareness training internally. According to PwC (2013), year 2013 saw a decline of staff dedicated to security awareness training program from 51% to 47%. There is also a decrease on amount of security consulting services. E&Y suggest that organization should never stop training their employees about what happened in the past and what are the risks and potential attacks around the corner. Besides, when entering a new market where all the factors such as security culture, business process, suppliers and vendors might be different than previous ones, employee should get familiar with security regulations, as well as policies in order to comply with government and security environment (E&Y, 2013).

Generally, arming people with up-to-date knowledge and skills is vital for the organization to become stronger internally. Information security awareness is not only limited to know-how but also an accurate sense of cyber risks and effective behavior towards cyber breaches.

3.5 State-of-affairs of 2012 information security surveys

There are 17 online-accessible information security surveys reports found in 2012. Among those, 4 reports focus on global information security situation, 1 report focus on health industry security situation, 2 surveys focus on smart grid security and challenges and 4 reports have explored the regional cyber security issues such as in Australia, Netherland, Kenya and Thailand. The rest have been written with specific topics such as cyber security survey for small business (published by Lancaster University), employee security awareness survey (Trenton Bond, 2012) and "a survey of computer and network security support from computer retailers to consumers in Australia" (Patryk Szewczyk, 2012).

Most of security surveys have implemented similar survey methodologies as previous years. E&Y and Kaspersky both have included more than 1000 companies, other surveys have investigated around 500 companies. Respondents came from main industry such as finance, manufacturing, energy, technology and government. SMEs are the major participants in both global and regional surveys.

In 2012, the velocity and complexity of technology development brought huge potential risks for different businesses. With the emerging mobile devices uses in the workplace, companies are facing the challenges in security control and compliance of regulatory requirements. Kaspersky global security survey revealed that the serious problems such as software vulnerabilities and inappropriate use of corporate network triggered the security issues for instance "malware, spam and unauthorized attempts to penetrate the system" (Kaspersky, 2012). Meanwhile, budget constraints, insufficient understanding of security issues among employees also created obstacles for strengthening companies' information security capabilities and building efficient security programs. E&Y 2012 global survey concluded that although organizations have put much more effort in improving their information security capabilities, they failed to keep up with the trend.

Through the review of 2012 cyber security survey reports, the following topics have been addressed seriously:

- Compliance management
- Security culture
- Training and education for improving understanding of security issues
- Data security (leakage and loss prevention) and
- Integrated strategy

The first topic is about company's compliance with security policies and regulations. According to E&Y (2012), "strong adherence to regulatory requirements" is vital for managing organization's information security risks. Many organizations have security policies and regulations to ensure quality of overall security practices and performance. However, having a written document is not enough; contents must be implemented by the entire organizations to enforce employees' secure behavior in daily operation.

According to Kaspersky report, one-third of respondents have lack of security control over mobile devices. Besides, 10% of respondents admitted that they have been experienced data leakage and loss during the last 12 months. This emphasizes the importance of strengthening organization's compliance with security regulations and policies.

Statistics from PwC's survey shows that less than half of respondents were actively monitoring and measuring their level of regulatory compliance. In CSI report, 66% of respondents admitted that compliance with regulatory requirements has positive effect on their security program. Specifically, 64% of respondents think their organization's security has been improved. Around 48% think it has affected the priority of security in the higher-level management. E&Y also mentioned 80% of their global survey respondents are aiming for compliance with regulations and it has become the important topic in board-level operations since 2005. Obviously, compliance can help enterprises to prevent the potential cyber threats through constantly measuring inside vulnerabilities. This plays significant role in finance and government sectors since they contain most valuable information from both business and nation side (E&Y, 2012).

Despite the fact that there are existing different laws, regulations, policies for business cyber security, companies should evaluate and identify the suitable ones and leverage them as a management tool to strengthen internal security situation. Specifically, company should take a complete look at which industry they are performing, what kind of information security regulations they are required to comply with, and what is their legal and contractual responsibilities in that specific area. Meanwhile, company should also comprehend the practical operations which those policies and regulations instituted.

Besides compliance with standard security policy, companies should also define an organizational information security policy for internal management. According to Backhouse and Dhillon (2011), there is no point to measure IS security if users do not comply with IS security policies. However, user noncompliance has become the big problem in today's organizations and there is a need to innovate new training approaches for improving this situation. Puhakainen and Siponen (2010) have proposed a new training program which is based on two theories for enhancing employees' compliance. Their model suggests that information security training should include both content and methods in order to "motivate the learner to systematic cognitive processing of information they receive during the training". Meanwhile, it is important to understand how employee perceives security issues before starting to improve the situation.

Another topic that has been discussed by most of cyber security survey in 2012 is the organizational security culture. It is known that information security is far more than technology control over Internet and corporate information. Yet, information security solutions have been developed to protect organization's information assets. However, organization may not be able to protect the connectivity, integrity and availability of information system if employees do not understand their roles and responsibilities in information security. Thus, it is vital to adequately train employees as well as create organizational information security culture in order to enforce the secure behavior in daily tasks.

PwC's report points out that in 2012, 95% of large organizations have implemented information security policy. By contrast, only 63% of small organizations have documented formal policy compared to 67% in 2010. Meanwhile, small businesses are more likely to rely on word of mouth rather than a defined policy. Only small amount of them ensure that their staff fully understand the security policy that has been designed for the organization (PwC, 2012). PwC report emphasizes that formulating the organizational way in handling security issues is essential for staffs to remind themselves their roles and responsibilities in protecting organization's information. Meanwhile, it can help them understand what potential security risks lie in daily business operation and how to deal with cyber breaches when they occur. Besides, constantly fostering and driving a security culture will help the organization to achieve its business goals efficiently and become stronger in the information security society (SANS, 2010).

Security training has been again addressed by 2012 cyber security surveys. Kaspersky report revealed that limited budget, insufficient understanding among senior managers and inadequate trained staff are constrains for achieving security objectives. Around 31% of respondents stated that senior managers do not see cyber security as significant threats to their business. 37% cited budget holders do not have adequate understanding of IT security. This implies that information security specialists are not only facing the technical problems but also responsible to convince the management and make them understand the importance of corporate protection against cyber security breaches (Kaspersky, 2012). Besides, PwC mentioned in their report that a customer of a large telecom company has suffered computer virus, however, the service provider ignored the problem and viewed it as customer's own mistake. After that, customer was still affected by virus and was given only little assistance by the company. This shows how senior management has poorly perceived cyber security issues, and how little they understood about the security policy (PwC, 2012). E&Y stated that resources alone couldn't support information security but also skillful personnel and profound understanding of cyber security issues among board-level executives. Thus, security training must meet the evolving changes and include all layers of employees in order to inform them about their roles in keeping organizational information security safe (E&Y, 2012). Meanwhile, SANS report suggest that training should include specific topic such as phishing and zero-day vulnerabilities in order to teach the internal staffs about how to securely use IS in their daily work. This can limit the security problems (SANS, 2012).

Today, huge amount of valuable data creates opportunities for businesses; on the other hand, it also brings potential threats and challenges for companies to keep their businesses secure. Data security refers to "protective digital privacy measures that are applied to prevent unauthorized access" to sensitive data which is normally saved in computers, databases and websites (Techopedia.com).

Kaspersky's report reveals that data breaches and loss of data increased from 30% to 35% between 2011 and 2012. Among those, 31% of respondents stated that some of their staff's action caused data leakage. 29% of respondents have experienced the loss or theft of mobile devices from company in 2012. Manuel Giralt Herrero from IT risk and assurance service in E&Y said, "organizations need to readjust their thinking from protecting the perimeter to protecting the data" (E&Y, 2012).

Indeed, the focus on data security protection can separate the companies from their competitors. Statistics from E&Y shows that around 72% of respondents have defined specific policy regarding the classification in handling sensitive data. 68% of respondents have implemented security awareness training and more than half of respondents have implemented additional security mechanism such as encryption. However, when looking at other protection methods such as using cloud services for saving company's information, the situation is worse than expected.

In PwC report, 73% of large organizations in 2012 have used Internet to save both highly-confidential and confidential data, so does small organizations (74%). Meanwhile, there is a trend for small company to save critical information in third party cloud services. PwC concluded that large organization is more likely to use outside resources to drive their business innovation. Meanwhile, with the emerging use of mobile devices in the workplace, companies are facing more challenges in data protection. 82% of respondents in PwC report allow personal mobile devices to connect to company's system remotely and this has dramatically changed over last two years. Cyber security assessment in Netherlands mentioned that employee should be responsible and liable for connected devices that are used only for personal and business purpose. Besides, organization should design strict rules for mobile users in the workplace to monitor the BYOD situation.

Whatever may be coming, organization should combine both technical protective measures and non-technical prevention approaches to manage their data security.

The final topic in 2012 is integrated security strategy which refers to an integration of company's information security strategy and business strategy with the purpose of obtaining holistic view of organization exposure (E&Y, 2012). Symantec report "Integrated security: creating the secure enterprise" point out that when the company's business become more sophisticated and dependent in the areas of business transaction, external data sharing and daily business communications, the need to access corporate business information has increased. Therefore, company must ensure authorized access to critical information. Yet, current information security solutions typically contain multiple products but lack of interoperability and manageability. So, it is essential to implement an integrated security strategy that is comprised of multiple security technologies which can be implemented to protect information in different functions of business. This way organization can reduce the costs of purchasing different security solutions while efficiently manage security issues in different units.

Based on E&Y's report, only 18% of respondents combined information security with their organizational business strategy in 2008. By 2012, this number has increased to 42%, almost close to half of their survey population. Since organization's reliance on information security function will not increase as much as core business, security function and particularly, security strategy should deliver maximum possible results to support the core functions and become a part of overall strategy.

3.6 State-of-affairs of 2011 information security surveys

There are 8 online-accessible information security surveys found in 2011. E&Y, PwC and CSI conducted their survey for exploring global cyber security situation. Carnegie Mellon University has published 2011 cybersecurity watch survey for United States, which shares the same regional focus with Ponemon Institute's survey. (ISC)2 has released global information security workforce study and another survey from PwC focus on global economic crime. Besides these, Cisco has published 2011 annual security report. The Parliamentary Office of Science and Technology in United Kingdom has released cyber security overview in UK in September 2011.

As for the survey population, E&Y has included nearly 1700 organizations in their survey across all major industries. CSI received 351 survey responds mainly from consulting, education, financial services, information technology, federal government and health services segments. PwC received more than 12,840 responses from CEOs, CIOs, CFOs and other directors in IT and security function from 135 countries. Most participants in 2011 global cyber security survey are large and small organizations.

With the recovery of global economy, more and more businesses start to adopt the digitalized globalization triggered by emerging technologies. With a significant increase in using mobile devices to carry and transfer data over the Internet among business partners, the traditional boarder of organization start to vanish, and the business world become more "borderless" and integrated. However, such a profound effect has also brought unknown dangers to digitalized business and significant impact on their perception of information security in this borderless environment (E&Y, 2011).

During this time, companies have witnessed a huge increase in both external and internal security threats. According to E&Y's survey report, 72% of respondents have seen an increased external threat. FBI reports in 2011 shows that more than 350,000 complaints of cybercrimes have been received, those have not even included unreported cases. Uscollegeresearch.org presents that 73% of United State and 65% of global Internet users have suffered victimization from cyber criminals through June 2011. Correspondingly, more than half of the respondents in E&Y's survey will increase their investment in information security function in the following 12 months.

Although evolving technologies are coming with unprecedented benefits and opportunities, companies are required to equip themselves with a well-thought security strategy to response to changes. Based on review of 2011 cyber security survey reports, the following topics have been frequently investigated and analyzed:

- Security policies for using trending technologies in workplace (cloud, social media, BYOD)
- Information security capabilities

The connected business world requires business to have right mixture of technology and security policies in order to benefit from the combination (Cisco, 2011). The rapid adoption of mobile techniques, cloud and social media in today's organizations triggered a fundamental change in information security policies. According to E&Y's statistics, about 57% of organizations have made policy adjustments in 2011 followed by 53% that have increased their security awareness activities through the year. Since the trend of using mobile techniques and digital devices in workplace cannot be avoided, Cisco annual report mention that it is essential to "find a common ground" where company understand individuals' needs while enforce them to comply with organizational rules in order to keep save of critical information and data.

Nowadays, an increasing number of companies start to support employees-own devices instead of providing preconfiguration for them (E&Y, 2011). This creates potential risks that employees may unknowingly make changes in those devices. Besides, mobile users may also remotely access to social media and cloud services for work purpose. This contains possibilities to put company's data to public and thus result security in danger. Based on these situations, Cisco suggests that no matter how enterprises perceive using emerging techniques in business operation, it is all about "policy elements in the interaction". If data is secured with technical control and loss-prevention tools, and employees are aware of critical security issues, it is not an endpoint for businesses. What's more, updating and adjusting security policies should also come along with educating and training employees about the risks associated with different devices. E&Y also suggest that organization should "perform attack and penetration testing on mobile apps before deployment to help reduce the organization's risk of exposure".

Cloud computing brought us new approach to save and backup data. The number of users of cloud computing-based services has increased slightly from 23% in 2010 to 36% in 2011 (E&Y, 2011). 9% of enterprises in Ponemon's survey have plan to spend their most IT dollars in cloud security in following 18 months. This is understandable since cloud services are still evolving and most of potential consumers have just started to recognize its efficiencies and convenience. However, there is no doubt that this compelling technique will be soon adopted by fast-evolving digital business and they must fundamentally change their security policy and "appetite" of partnering with external service providers in order to deploy it successfully. Cisco suggest that companies should establish a classification system for the data such as "public", "confidential" and "high confidential" in order to be clear what information can be uploaded and shared in cloud with others. Meanwhile, choosing a reliable service provider who has strict security rules and who is critical about security issues can significantly strengthen the data security, since they assess vulnerabilities more seriously than others.

Social media is an emerging way for business to connect with customers. It not only allows company to keep contact with customers but also develop business through media marketing and follow up customer feedback. However, statistics from global survey shows different situation on adopting social media.

E&Y report presents that 53% of respondents have limited access or no access to social media websites. Only 46% of companies have adjusted their security policy for this new marketing approach. Some key findings from PwC's survey suggest that many companies are unprepared for the potential risks brought by social networking. There are only 32% of respondents in United Kingdom who have implemented some technologies for supporting Web 2.0 information exchanges such as blog, social networks, wiki and so on (PwC, 2011).

As a result, companies that are not equipped with profound understanding and effective adoption on social network and other Web 2.0 platforms can easily expose to cyber risks. (PwC, 2011). Besides, malware from social media has also caused security breaches in 29% of companies in Ponemon's survey. Because of these reasons, it is more common to see some easy way or hardline reaction towards social network than active adoption (E&Y, 2011).

Nevertheless, all these developing technologies are two-side sword. It is more important to consider how to embrace and monitor these tools in new digitalized business rather than totally avoid them. E&Y suggests that in order to fully leverage the advantages of social media, organizations may reform their perception of it and adjust the internal security policy to enforce personnel who use this technology in secured manner.

The next topic is about cyber security capabilities in combating sophisticated cyberattacks. No matter what size the company is, all should equip with some cyber security capabilities to keep their information away from attack. Large organization may have structured and well-organized security department while small organization may have limited security resources and insufficient spending and workforce. With complete and matured cyber security capabilities, company can defend some breaches in advance and protect them against large sabotage from cyberattacks. PwC report (2011) reveals that security executives complained that their company has restrained the spending which often result on degradation of fundamental security capabilities such as employee background check and use of vulnerability assessment tools. Hence, both PwC and EY report addressed that in-house cyberattack defensing and preventing capabilities are very weak among investigated companies. 60% of companies in PwC report think their in-house capabilities to prevent and detect cybercrime is adequate (PwC, 2011). Less than 4% in EY report stated they have increased funding in incidence response capability development in the following twelve months. On the government side, most of reports found focus on building nation-level defensive cyber security capability. There was no comprehensive assessment defined for measuring cyber security capabilities maturity. This shortage does not help companies to compare themselves with others nor to find their vulnerabilities. Meanwhile, decision maker also has no better way to analyze what is vulnerable inside and decide how to support the capability development.

3.7 State-of-affairs of 2010 information security surveys

There are in total 12 survey reports focus on 2010 cyber security situation. Among those, 7 reports focus on global cyber security situation, 3 reports focus on regional computer crimes and security issues and other 2 reports have investigated data security and privacy situation in Indian bank industry (KPMG, 2010) and security issues in service delivery models of cloud computing (Subashini and Kavitha, 2010). The number of participants is ranging from 500 to 7,000. E&Y, PwC, Symantec and CSI have received more than 1,000 feedbacks from business and IT executives across major industries.

With recovery of economies from downturn and emerging technologies blurring the lines of traditional business, companies start to embrace a new age of technology, information, people and security.

According to Symantec Global 2010 SMB Information Protection Survey, more than half of respondents rate the data loss as the risks which has greatest significance to their organizations. Statistics from 2010 Inforsecurity Europe shows that 92% of large enterprises had experienced security incident during 2010 compared to 72% in 2008. The average cost of incidence ranging from 280,000 pounds to 690,000 pounds. Meanwhile, small organizations that have less than 50 employees also suffered from cyber breaches. 83% have experienced cyber incidence and the average cost is double than 2008 which was 10,000 to 20,000 ponds. Around 40% of respondents in Symantec report think enhancing their backup, recovery and ability to resume computing as quickly as possible after cyberattacks are important IT improvement areas for 2010.

Given the fact that 2010 has been shaped by cyber breaches as a dynamic year, companies are urged to take a holistic view on their security practices. Based on review of 2010 cyber security survey reports, the following topics have been addressed intensively:

- Data Loss Protection (DLP)
- Information security training and
- Compliance with security regulations and standards

E&Y defined data leakage or data loss prevention as "the combination of tools and process for identifying, monitoring and protecting sensitive data or information according to an organization's policies or government and industry regulations." The primary focus of data loss prevention is preventing the critical data leakage from organization by controlling the unauthorized access and transmission of confidential information to other parties or individuals. Based on statistics in Infosecurity Europe report, 48% of respondents have suffered few cyber incidences in confidential information loss and leakage. 54% have experienced the staff-related incidence for example unauthorized access to systems or data. Similarly, Symantec report reveals that when respondents were asked to rank different business threats, SMEs rated data loss and cyberattack as the top priorities followed by traditional criminal activities and natural disasters. In some cases, SMEs have even spent more in information protection than other functional tasks (Symantec, 2010). This implies that crucial information loss is a real threat facing the recovering business; and safeguarding the information assets is the top mission for all types of enterprises.

DLP tools or solutions are the primary tools to help companies to deal with information leakage problem. Securosis defines DLP tools as "products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis". Data at rest means documents that have no usefulness and have been saved as backup resources. This is a common case for businesses and government and those backups have high potential to be stolen or accessed by authorized individuals. Data in use refers to the active data which is stored on systems that users are currently interacting with. Unauthorized activities can be easily found by DLP system such as through screen-capture, analyze print or fax that include sensitive data. Data in motion refers to those moving emails through a network to an endpoint. DLP solutions ensure that the data reaches safely to the destination.

Statistics in Infosecurity Europe report presents that many organizations have adopted strong authentication and encryption techniques to secure their data. 75% of large organizations and 57% of small organizations have encrypted laptop and hard disks. However, there are in total 23% of enterprises hold encryption on virtual storage such as cloud services, which triggers the question of how to control the data security when using third party services. Pwc reveals that only 23% of organizations have ability to enforce provider security policies. 22% stated that they have insufficient training and inadequate IT auditing. Although jumping into cloud and replacing server room can improve efficiency but rushing without a specific security strategy can bring unexpected risks to organizations (PwC, 2010). Chris Hoff from Cisco System recommend that both customers and service providers should ensure that they understand risks associated with new technologies and be aware of changes brought by these new innovations to organization, technology and operation functions (PwC, 2010).

Based on this situation, Symantec report suggest that companies especially SMEs should implement a comprehensive and complete DLP solutions in order to keep their own right to customer privacy information and enterprise business information. Besides, educating and improving employee awareness toward security risks are significant for protecting data security internally.

Information security training has been again addressed by most 2010 cyber reports. It is a clear trend that technology controls are not enough to keep company's information security safe. A good combination of human resources, technology and strategy is now required to support entire business data security.

42% of respondents in E&Y survey state that their employees' awareness of security has been a practical challenge followed by 39% who think skilled resources are critical for security maintenance. Nearly 50% of large enterprises in Infosecurity report have experienced leakage of confidential data, which was caused by internal staff. However, the positive side is that 57% of investigated companies in PwC survey have monitored employees' behavior by using online assets; and this figure has increased 20% between 2006 and 2009. Meanwhile, 36% companies have checked what employees post on external website such as blogs or social media websites.

As the mobile usage grows and internal threats increases, companies start to realize the significance of security awareness training in preventing harmful damage to them.

E&Y suggests that business should re-engineer their security strategy incorporated with innovation adoption plan so that employees can leverage these resources to handle their tasks while encrypt the confidential data without being exploited by cyber criminals (E&Y, 2010). In addition, organizations should never stop training and educating to ensure their employees fully understand the security policy and bear in mind the insecure behavior for example misuse of Internet or email, less update of IS, negligence of suspicious malware and so on.

The next topic is security regulation compliance. Luckily, there is no doubt to put compliance with regulation as one of the priority tasks in organization security initiatives. 56% of respondents in E&Y report think achieving compliance with information security regulation is important for supporting security activities in organizations. In 2010 Financial Services Global Security Study, for the first-time investigators have seen security compliance among top-five initiatives for gearing up organization's security situation. Around 20% users in New Zealand 2010 cyber security survey have adopted different security standards such as ISO/IEC 27001/27002, SIGS (Security in the Government Sector), AS/NZS ISO/IEC 17799 and vendor-specific standard.

Needless to say, compliance can make the overall organizational environment more under control which means guidelines, rules and practices procedure are being followed by all the functions. Meanwhile, it can create a chain of responsibilities so that everyone in this network have certain responsibilities to enforce the compliance and testing the control. This can facilitate security culture and strengthen the internal security infrastructure against outside turbulence.

3.8 State-of-affairs of 2009 information security surveys

There are in total 16 computer security survey reports captured in 2009. Among those, 9 reports focus on global cyber security situation, others have explored the computer security from different perspectives such as crime victim, cyberattack detection system, retail crime, identity fraud and so on. The number of participants in global investigation is ranging from 90 to 1900. Respondents represented diverse industries and companies. Financial services, manufacturing, telecommunication, technology, retail wholesales and distributions, energy and media are the popularity in most of investigations. Most respondents come from European countries, Asian pacific countries and American countries. Middle East and African countries remain 4% to 9% in global surveys.

It is known that the year 2009 has seen the most difficult time for business in 21st century. The global economic crisis hit many businesses hard and brought them new challenges in finance, information security, human and technical resources and customer loyalty. The increased pressure of reducing business expenditure, protecting business and customer information, as well as increased government and industry regulations force the companies to seek new ways to work and reinvent themselves in this turbulent business environment (E&Y, 2009). Meanwhile, a bunch of new technology innovations jump into the business-centric view and bring both opportunities and risks to organizations.

Based on 2009 annual report published by PandaLabs, there has been a new historical record of phishing and malware appeared in 2009. Their figure shows that the most prevalent malware in 2009 was Trojans, with 66% cases reported at PandaLad compared to 17.2% of adware, 6.61% of virus, 5.7% of spyware and 3.42% of worm. Meanwhile, according to CSI Computer Crime and Security Survey, 64% of respondents have suffered malware infection in 2009 compares to 50% in 2008. FBI identified that spear phishing attacks loss was 100 million dollars in 2009 United States business (Quarterly Security Statistics Review, RSA). As for the global consequence of malware and phishing, many countries from East Asia, Central Europe and North America have been hit by the storm. Based on PandaLad report, Taiwan (62.20%), Russia (56.77%) and Poland (55.40%) are the top countries that have been infected mostly by malware. Other countries such as United States, Brazil, Italy, France and Chile have approximately 50% infection rate. Obviously, malware attacks are mostly financial-oriented; it has been a quick and simple way for cyber criminals to obtain money from stealing bank detail information (PandaLab, 2009). Besides, the popularity of social website such as Twitter and Facebook have also become the valuable tool for cyber-crooks to propagate the malware and spam over the Web 2.0 users. Social networking, as an important tool facilitates people's virtual interaction, presents also many potential risks and threats to vulnerable businesses.

Based on this situation, information security leaders start to analyze and understand the important factors that will influence the reshaping and reconstructing of their companies' businesses. There has been a growing concern in following topics among 2009 cyber security survey results:

- Privacy and personal information management

- Technical and non-technical controls of cyber risks such as spam, malware, phishing and potential threats of social networking

With the crash of economy, the challenges of new technologies such as social media and cloud computing, protecting personal data and privacy of customers became a focus in information security management. Today, organizations can explore potential markets and target groups by collecting personal data through Internet. Meanwhile, millions of customer private data has been received by companies through software applications and through websites without any guarantee that this data will not leak to third parties. In response to this situation, governments have passed privacy laws considering protecting personal information from disclosure, transfer and sale. Companies are required to comply with these laws and build their information security infrastructure to protect customers information (SANS, 2002).

According to E&Y 2009 global state cyber security report, 53% of respondents state that managing privacy and protecting personal information are the important activities supporting organizations. About 68% of their respondents say that they have understood clearly the privacy laws and regulations which may impact to their business. 63% have included privacy requirements that are designed when partnering with external suppliers, vendors and contractors. Although privacy issues are necessary part for businesses to consider especially in today's explosion of information and security crimes, E&Y report reveals that only few of organizations have implemented a process to monitor and maintain privacy-related concerns and problems (E&Y, 2009). Only 26% have concluded the assessment for the personal information life cycles. Less than 40% of respondents covered their inventory of critical data by privacy-related regulations and requirements (E&Y, 2009).

On the other hand, security concerns among customers and a large amount of stolen information from different websites, information systems and software applications ring the bell in organizations. RSA 2010 global online consumer security survey reveals that around 90% of customers worried about their personal information being accessed or stolen by external parties from online banking services. Nearly all the service consumers were expected monitoring measures from online bank on their online transactions. Moreover, based on "Chronology of Data breaches" from Privacy Rights Clearninghouse which is a non-profit organization that advocate consumer information, "260 million personal records were reported lost or stolen since January 2005 just in United States" (Cisco 2009 Midyear Security Report). Theft Resource Center (ITRC) also reported that the amount of data breaches was doubled in 2008 than 2007, and 15 million personal records were reported to be stolen within the year 2008 (Cisco 2009 Midyear Security Report). Indeed, privacy concerns have expanded widely and deeply into the worldwide organizations. How to bring confidence to customers through companies' data security practices becomes a sophisticated challenge.

Needless to say, technology has made success in protecting data against leakage and stolen by outside exploiters, however, concrete privacy rules, legal environment and effective security awareness training are also critical for protecting data. SANS report "Using security to protect the privacy of customer information" pointed out that an effective privacy policy should be "clear, concise and lawful to express the best interest of its customers". The policy makers should clearly explain in what situation customer data will be saved, for what purpose and in which situation this information will be shared with other parties for the purpose of products or services research (SANS, 2002). Customers must obtain detailed information and own the right to make choice of what information can be shared, with whom and for what purpose. Since customers are unaware of how companies deal with the provided information from them and worry about this sensitive information being accessed by others without authorization, companies must "identify all personal information and limit the access on a need-to-know principle" (SANS, 2002). Besides, a legal environment can influence the organizational infrastructure and information security practices in daily business operation. Currently, there are two most-known federal legislations focusing on the transmission and storage of customers data: HIPAA (Health insurance Portability and Accountability Act) and GLBA (Gramm-Leach-Bliley Act). The first one is related to health information and health insurance data protection; the second one focuses on ensuring financial service industries such as banking, investment institutions and insurance to protect customer private information. Before information security professionals and IS executives design and implement the IS security solution, organization must clearly understand these legislations and the legal environment in which they operate their businesses. Meanwhile, these acts also ensure that organizations disclose their privacy policies to customers and describe how they use and share the nonpublic data so that consumers can be informed about their privacy and information security. Another important part is to promote the training and education to employees concerning illegal and unethical behavior towards data protection. Sometimes the case is that security professionals fully understand those acts, regulations and requirements when handling sensitive information, but employees are unaware of and underestimate those policies and legal procedures. Therefore, security professionals should safeguard the information from both technical and non-technical parts.

Generally, defense of cyber threats today requires multi-layers initiatives. Business should combine the policies with technologies to address the privacy issues and maintain customer confidence especially in global economy turbulent time.

The second topic that has been discussed mostly is the management of cyber risks such as spam, malware, phishing and potential threats of social networking by using both technical and non-technical methods. With the wide adoption and use of Emails, a modern electronic communication tool for private users, businesses, governments and other institutions, email system has been also received attention by cyber-crooks. In recent years, huge volumes of spams, bulk emails, fraud and other security threats have assaulted many email-users. According to Email Statistics Report 2009-2013 published by The Radicatic

Group, approximately 81% of total email traffic was spam emails in 2009. Private users feel annoyed by spam, but for organizations it is considerable expense (The Radicatic Group, 2009). The report shows that organizations that have 1000 email users might spend 1.8 million dollars a year to manage the spam. Meanwhile, nearly all investigated users in ENISA 2009 spam survey think that managing spam are "significant" part in their daily information security operations. Indeed, spam can influence the user experience, and this is harmful for company to deliver high quality products or services and maintain customer relationships. However, due to the limited budget and size of businesses, anti-spam investments vary greatly, from 10,000 annually to millions in some large enterprises (ENISA, 2009). How to manage this cyber risk efficiently and effectively becomes a challenge for many service and product providers. Beside spam, malware, phishing and virus there are other critical information security problems faced by organizations. As mentioned above, technology shift and downturn economy fueled the increase of external threats to business between 2008 and 2009. Half of respondents in E&Y's survey indicate that they will spend more money on improving information security risk management in next year followed by improving data loss prevention solutions. Since risk management is an ongoing process and need to be supported by both technology and human resources, some surveys mentioned following perspectives concerning the better improvement.

ENISA report reveals that many originations see spam prevention with a great significance. When a company successfully managed the spam and implemented anti-spam prevention methods, this can become a selling point to customers and a competitive advantage to its competitors. Meanwhile, there are many technical measures for detecting and against spam messages; for example providing network-based spam filtering to customers to prevent them receiving the spam, using blacklist to measure and prevent sending of spam, analyzing the spam resources based on receipt of customer complaints or using anti-spam software. As for the non-technical approach, Freitas and Levene (2004) suggest the legislative method to prevent spam in the future. However, this depends largely on the agreement of all the nations in the world and collaboration for enforcement.

As for malware and phishing, they often come together. For example, "the phishing email may contain links to websites that are infected with malware" (Wikipedia, Phishing). Besides, cyber criminals can entry into the IT systems through phishing attacks and then spread out ransomware and impact the entire IT infrastructure. US-CERT report "Technical Trend in Phishing Attacks" listed several technical and non-technical solutions in response to this situation. For example, awareness and education can raise both customers' and employees' attention of phishing. Particularly, employees can explain and answer to customer's question if they are knowledgeable about phishing threat. Besides, leveraging the law enforcement to shut down the website can benefit all the companies that have received the phishing emails from that website. Moreover, a common way for normal users to prevent the phishing and malware is to a safeguard web browser toolbar which can identify if customer is viewing a possible phishing website.

Social network has been criticized by many survey reports in 2009 since it became a new way for cyber-crooks to spread out malware. Based on Panda Labs annual report, Twitter was used by cyber criminals as an information pool to define the target. Since people can use the "Twitter Trends" function to check the most popular topics on Twitter, their focus of interests might be used as baits that link them to another website which contains malware. Meanwhile, it has occurred that some other website has been imitating Facebook and designed to steal user's account information. Indeed, end-users are the most vulnerable part in information security chain. Besides using anti- software, both private users and organizations are recommended to have strong awareness and vigilance when encountering cyber threats. Employees should constantly evolve their capabilities in identifying malware, phishing and virus attack and customers need to be aware of increasing sophisticated technical deceits and financial impact from installing the malware on their computer (US-CERT, 2012).

Generally, risk management requires company to understand the potential threats and risks, assessing the impact associated with those and exploring suitable ways to remediate them over time. Acquiring more IT professionals with the profound experience and knowledge in risk management can significantly support this process and strengthen the internal IT infrastructure. Meanwhile, increasing user awareness and following the trend of technology development can decrease the likelihood of cyber breaches~~,~~ and maintain profitability.

3.9 State-of-affairs of 2008 information security surveys

There are around 15 online-accessible computer security survey reports in 2008. Among those, 8 reports have explored global state of cyber security, 7 reports focus on local information security situation in United States, United Kingdom and Australia. Other reports have analyzed the HIPPA (Health Insurance Portability and Accountability Act) compliance among the entities covered by policy which are health care providers, health plan and health care clearinghouse (hhs.gov). The number of participants in global investigation is ranging from 20 to 7,000. Beside a survey from Deloitte that has investigated cyber security practices only in Technology, Media and Telecommunication (TMT) industries, other surveys have examined major industries such as financial services, information technology, health services, government and manufacturing. Most participants in global survey are medium and large size organizations with 1500 to 9999 employees and over 1 billion annual revenue. Most of respondents in global surveys are CIOs and IT executives.

According to Cisco (2008), the "top concerns of 2008" was "blended threats that combine email and websites and use social engineering techniques".

The downturn of economy has not only influenced business but also brought new threats and risks towards corporates information security. Although many reports reveal that the investment are not being reduced, organizations are uncertain if these investments has been put in right place and how can business case justify their expenditure. On the other hand, information security has improved driven by technical threats, but organizations still struggle with aligning security with business and achieving a strategic view of cyber security. Moreover, human factors continue being addressed by many surveys reports as "the weakest link in the security chain" (E&Y, 2008). This implies that no matter how much investment organization have made in technology, there still a need to train people on what to do and how to do in order to achieve the investment goal. In general, cyber security has gained sophistication with various new types of threats, emerged techniques and obstacles in learning and understanding how to implement technologies by organizations. These challenges require companies to ensure the basic things done correctly, look beyond existing data, plan for uncertainty and strengthen the capabilities for the upcoming battle based on the review. The following topics haven been addressed mostly by 2008 cyber security surveys:

- Information security investment
- Human factors in security chain
- Management of information security outsourcing

As mentioned above, businesses are keeping investing in information security during the turbulence of world economy. According to E&Y's report, only 5% of respondents state that they will reduce the annual expenditure in cyber security. BERR 2008 information security breaches survey also shows that "the average expenditure on information security continue rise" with 7% of IT budget spending on information security by SMEs, compared to 4%-5% in 2006. However, it is difficult to ensure a better security with only investment, and many reports also indicate that companies are not specifically tracking their security investment. For example, only about 29% of respondents in TMT survey published by Deloitte believe that their expenditure has been used in the right target. Just about 20% of respondents have documented security investment strategy in E&Y's report and less than half of them perform the risk analyses activities to check the effects from security investment.

On the other hand, CSI 2008 computer crime and security survey reveals that senior management do not easily approve the investment in cyber security strategy, instead, some organizations like to use economic terms such as Return of Investment (ROI), Internal Rate of Return (IRR) and Net Present Value (NPV) to measure the benefits from investment in order to make wise decisions based on the "fact". Their figure shows that the number of respondents using financial terms in their security decision has increased steadily from 2006 to 2008 (CSI, 2008). Obviously, decision maker can obtain detailed information by checking the potential financial loss and the costs to preventing those, however, CSI report says that this cannot be the "predominant domain in the current decision-making".

Besides, the existing works in researching economics in information security investment also present different aspects to determine weather the investment is worth to be made based on company's risk appetite, financial resources and business objectives. Gordon and Loeb (2002) point out that organizations should focus on protecting the midrange vulnerabilities since the information sets with highest vulnerabilities "may be inordinately expensive". Huseyin, Srinivasan and Wei (2008) suggest that traditional risk assessment is not sufficient to support the investment decision-making. They proposed a "game theory for determining IT security investment levels on several dimensions such as the investment level, vulnerability and payoff form the investment". They also found out that firms could learn from their prior experiences being hacked and make decisions based on those.

Indeed, the view of information security investment varies in different companies. In order to receive benefits at the maximum level, organization should establish a long-term objective combined with clear information security strategy and integrated risk management approaches (E&Y, 2008). Meanwhile, PwC 2008 global state cyber report mentions that information security executives should understand well what contribution the organization expect from information security investment and have they been achieved. If the answer is no, then they need to find out if these investments has been properly aligned with their business objectives.

In addition, PwC report also addresses that organizations have not fully understood their investments in advanced technologies that are designed to protect sensitive information. Although most of investigated organizations have encryption of laptops, databases, file shares, backup tapes and removable medias, as well as web or Internet content filters, different detection and protection tools, they still do not know where the most critical and sensitive information is located. This hinders them capturing the benefits from technologies that are intended to support the business from security, privacy and compliance perspectives.

Therefore, increasing security investments can be a problem if the organization does not know where the critical information sets and what are real information security challenges faced by them, and not just those typical attacks that are embedded with patterns which current developed technologies can easily identify and recognize (CSI, 2008).

The next topic is about human factors in security chain. Since more and more businesses start to realize that security issues, privacy risks and data breaches are not only influenced by technical environment but also human factors such as behavior and security awareness of employees, 2008 security investigations have addressed this topic seriously. Based on a data breaches report that has covered 500 breaches cases handled by the Verizon Business risk team over four-year period (2004-2007), only 18% of security incidences was caused by internal factors compares to 73% caused by external sources. However, this does not mean that internal threats are less significant than outside attacks, in fact, the trends in data breaches sources during these four years clearly presents that the rate of internal and external sources in security breaches have become similar, both are close to 44% (Figure 10). Statistics from PwC report presents that companies do not seem to know about the source of incidences. Nearly half of respondents (42%) in their report were not sure about this question: whether the cyber incidences are caused by internal staff, business partners, customers or suppliers? Meanwhile, 50% of organizations did not conduct the personal background check and about same amount did not monitor employee access of Internet and information assets.

On the other hand, Verizon's report discovered that IT administrators (50%) and employees (41%) are the two major source group of internal breach followed by executive (2%), agent or spy (2%) and anonymous (5%). As one might suspect that IT administrators usually have more access opportunities than any other employees in the business, this privilege enables them to open a door to external groups and bring unpredictable damage to company's information assets and even business. Besides, the little amount difference between IT administrators and employees also gives a reminder that higher level of access is not the only reason for data breach. Employees' behavior and awareness of insider threats also bring positive or negative impact to the security risks.

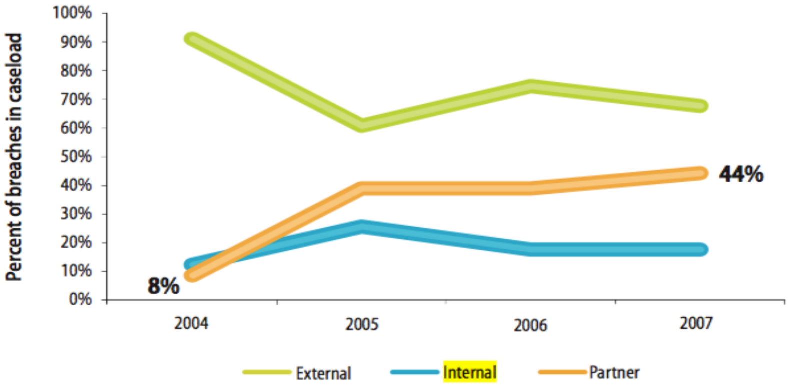

Figure 10. Percent of breaches in caseload

Implementing security awareness training is one thing; verifying employee understanding of security policy and measuring the effectiveness of training is another. According to CSI report, 36% of investigated organizations performed the mandatory written or digital test in awareness training about security risks and appropriate handling of data. However, also about same amount (32%) of them did not measure the effectiveness of security training. E&Y report shows that half of their investigated companies state that organizational awareness training is the "most significant challenge to delivering successful information security initiatives". 85% of respondents performed regularly the Internet testing but only 19% conducted the social engineering attempts to test their employees. Many firms do not recognize the risks brought by new technologies and therefore, are not aware of breaches involve from those (BERR, 2008). Meanwhile, CSI report says it is surprising to see that most of today's companies spent less than 1% of budget on security training. The reason behind might be the relatively low costs of awareness training; but on the other hand, it also reflects companies' "general cynicism about the necessity or effectiveness of awareness training".

Clearly, security training is a necessary part of the security agenda. Without training individuals with responsibilities of handling sensitive data about what to do and how to do, it is difficult to achieve the information protection objectives and long-term business goals. Meanwhile, E&Y suggest that organizations should view employees as critical as any other components in information security in order to control and prevent the incidences from inside since they are most prone to allows outside exploiters access internal information. Besides, a large number of researches on human behavior emphasize that behavior is the results from individual plus environment. However, without understanding employees' perception and knowledge of security issues, as well as their prior employment background, it is difficult to conduct an effective security training that leads the IS security and personal mastery of security responsibilities (Perry 1985).

Several surveys have included information security outsourcing topic in their investigations. With increased pressure from different customer demands in market place and limited financial, human and technical resources, many organizations turned to outsource a part of or whole IT infrastructure to outside service providers in order to leverage both costs and efficiency benefits. However, outsourcing is not as easy task as defining an outsourcing plan and strategy, researching a suitable service provider and making a deal with them. In fact, it associates with many potential risks and even problems; for example, the plan may not work as the company expected or information leak to third party. So, it is not just about calculating the costs savings, but also considering labor, technology and information privacy elements.

Based on BERR report, outsourcing remains common in 2008 with more than half of their survey respondents having outsourced some of their IT functions such as IS development, system administration and help-desk. Statistics in E&Y report also shows that 23% of respondents plan to outsource or enlarge the size of outsourcing in the following years. However, security issues were also raised by the increasing amount of outsourcing companies which had access to company's internal sensitive information. According to TMT survey (Deloitte, 2008), 56% of survey respondents have experienced the external data breach which was caused by "trusted" vendors. Verizon report also reveals that over 40% of cyber breaches were resulted by access and control and in most cases, the account which was intended to be used by vendors, but internal information was leaked to external parties. This implies that it is difficult for company that has outsourced the services to know who is using the authorized administration to access enterprise information assets and this vulnerability creates huge convenience for attacker to do their "jobs".

Thus, many corporates do not trust in outsourcing information security practices. Only a small amount of companies in E&Y have outsourced their incidence response activities (15%) and forensic investigations (19%). Even though outsourcing may bring both advantages and disadvantages to organizations, security reports suggest that business should look for balance between its own conditions and outsourced activities (E&Y, 2008). When preparing the outsourcing services, company should clearly define the outsourcing strategy, objectives as well as the security requirements such as what information can be accessed by service suppliers and how the service provider handle the personal and sensitive information. A service level agreement (SLAs) should be included in contract in which expected performance in security control by service providers, measurable outcomes and incidence response approaches and remedies are clearly defined (IT outsourcing security by the government of the Hong Kong special administrative region, 2008). When engaging external service providers, organization should regularly perform the security control based on their requirements and test and review the vendor's security capabilities in order to make adjustment before the occurrences stem (Deloite, 2008). Although organizations can choose to outsource different IT operation and security activities to third party, "the responsibilities and liability of any breach to sensitive or personal data remains entirely with organization" (IT outsourcing security, 2008). Meanwhile, organizations should also pay attention to employees who have assigned with responsibilities in handling sensitive data in vendor company and ensure they have adequate skills and knowledge, as well as strong awareness of cyber security incidences and breaches. Moreover, organizations should plan for uncertainty no matter how the third party practices are under control. Developing and rehearsing responses can effectively help organizations to react against cyber breaches in a timely manner and control the damage at a maximum level.

4 Findings

The finding part presents the categorized cyber security topics based on ISO/IEC 27002 standard. As mentioned previously, this thesis is a standalone literature review that aims to provide a holistic overview and in-depth analysis on critical cyber security issues in organizational security practices. Below chart clearly present the most vulnerable part in which enterprises have encountered cyber security problems. The outlined sections will be discussed in detail in the discussion part (Table 3).

Table 3. Sections of ISO/IEC 27002 and highlighted parts based on review

Sections of ISO/IEC 27002 Standard	
Sections	Topics
1. Risk management	- **Risk assessment (2010: data loss prevention)** - **Risk analysis** - **Risk mitigation (2012: data leakage and loss prevention; 2014: risk management)**
2. Security policy	- **Principles and standards (2011: Policy for using trending technologies in workplace)** - Procedure - Control and approval
3. Organization of information security	- **Internal structure (2013: board involvement; 2014: cyber security governance)** o Coordination and responsibilities o Agreement o Reporting - **External Structure (2008: man-**

	agement of information security outsourcing) o **Risks with external partners** o Security issues with new customer o **Third party agreement (2014: third party management)**
4. Assets management	- Inventory - Ownership - Authorized use of assets - Classification - Information labeling and handling
5. Human resource security	- **Prior employment (2013: technical skills of employee; 2016: IS constrain-insufficient IT security resources)** o Roles and responsibilities o **Screening (2015: inside threats)** o Terms for employment - **During employment (2008: human factors in security chain; 2016: IS constrain-employee related risks)** o Management responsibilities o Training and education **(2010: training; 2012: training and education; 2013: awareness training; 2014: human resource management; 2016: continuous training and education)** - Termination o Responsibilities o Return of assets
6. Physical and environmental security	- Physical equipment security - Secure area - Protecting against external threats
7. Communication and operational management	- Archives, logs, backups, patching, monitoring and configurations **(2009: Social networking threats; 2015: IOT)**
8. Access control	- User access management **(2009: non-technical control; 2013: administrative control)** - **User responsibilities (2009: non-**

	technical control) - **Network access control (2009: technical control; 2013: technical control; 2014: technical control)** - Operating system access control - Application and information access control - Mobile computing and teleworking
9. Information system acquisition, development and maintenance	- Requirement, design, development, test, implement, maintenance
10. Information security incidence management	- Reporting system **(2013: incidence response plan)** - **Responsibilities and procedure (2014: incidence response management)** - **Learning from incidence (2015: threats intelligence; 2016: cyber threats intelligence for anticipating risks)** - **Disaster recovery (2014: incidence insurance)** - Collection of evidence
11. Business continuity management	- **Including information security into business strategy (2012: integrated strategy)** - Business continuity and risk management - Implement security in business continuity plan

12. Compliance	- Identification of applicable guidelines - Protection of organizational records - **Data protection and privacy (2009: privacy management)** - **Compliance with security policy and standard (2010: compliance; 2012: compliance with regulatory requirements)** - Technical compliance checking - **Information system audit controls (2013: security audit and control)** - Protection of information system audit tools

5 Discussion

The discussion part will analyze the outlined topics in finding part from origin, components, obstacles and improvement perspectives combined with relevant academic literature. The purpose of this chapter is to understand why enterprises have performed less in those sections in order to highlight the focus of cyber security practices for industry practitioners for the future.

5.1 Risk management

Based on review, risk management is one of the most vulnerable parts in enterprises cyber security practices. The origin of risks comes from all kinds of interaction with people and access to the network (Lawrence et al, 2008). As mentioned in sub-chapter of 2014, today's information security risks associated with human errors, internal and external threats, advanced digital technologies, company's security infrastructure and management (Colwill, 2009; Stonerburner et al, 2002; Lawrence et al, 2008).

The components of cyber security risk management are risk identification, risk prioritization, risk mitigation and risk strategy (Landoll & Landoll, 2005). Risk identification requires enterprise to understand the cyber security landscape, find out what cyber risks associated with company's information and operations, identify the capabilities and process to defend risks and estimate the overall costs for recovery. This helps to prioritize the risks that are most critical and significant for companies without blindly defending different attacks. Risk mitigation can be achieved by improving cyber security awareness, continuous training and education about trending technologies and potential threat, and by keeping update the techniques such as encryption and strong authentication. By including the risks strategy into business management, organization can benefit from long-term support from higher level executives in security improvement. Meanwhile, the strategy defines the key responsibilities for vital functions and important tasks for entire organization for improve its capabilities in defending evolving cyberattacks.

However, through the review there are several obstacles in risks management development. The first important factor is the emerging technologies that brings both benefits and security issues to the companies when most of them have not yet fully prepared to leverage this double-edged sword (Tipton & Krause, 2007; Kuyoro et al, 2011). As mentioned in 2012 sub-chapter, many large organizations use Internet to save both highly confidential and confidential data, so does small organizations. However, the volume of using cloud services is putting data security at the risks. Although organization always keep searching the trustable service provider, threats from data access management, third party credentials evaluation and system vulnerability brings other security concerns.

The second obstacle is poorly defined cyber exposure. As review presented, today many companies are poorly identified their security appetite and information security assets from technology, database, intelligence and employed cyber security experts. It is hard to obtain a frim view on critical dependencies in long-term business without this information (Rok, 2008). Meanwhile, a limited understanding of potential risks will result in negligence of cyberattacks damage, which is particularly harmful for SMEs.

The third obstacle is insufficient financial support from senior management. It is observed that there will be no financial support arranged for cyber security issues unless company's main business is aligning with cyber security (E&Y, 2010; Symantec, 2010; PwC, 2012). Indeed, cyber breaches are no longer affect only IT functions but entire business. It is critical for decision makers to take cyber threats into consideration and prepare defense strategy before attack happen in order to keep company on the safe side (Rasmussen, 1997; Hong et al, 2003; Garg, 2003).

As for the improvement, according to IEC/ISO 27002 Standard risk management section, before treating the risks companies are required to have clear picture of which area cyber security risks are accepted and where not. Risks can be accepted if it has low impact to the business and cost of treatment is rather higher than recovery cost (Zhang et al, 2010). Secondly, for those identified risks company should make decision and plan for mitigating and controlling the impact from it. On the one hand, appropriate solution should be defined; on the other hand, insurance should be in placed to avoid disaster. It is also important to assess the value of different countermeasure and avoid one-fit-all solutions.

5.2 Security policy

According to IEC/ISO 27002 standard, the objective of security policy is to provide management and operation guidelines in accordance with business development goals and relevant information security standards, laws and regulations. Meanwhile, security policy should include clear management principles for achieving security target and business development objectives.

A good information security policy should include following components: a clear definition of security infrastructure together with security goal and responsibilities for each party, reference to other security policies, enforcement and control, update and improvement (Baskerville & Siponen, 2002).

When building a security policy for internal use, it must have clear definition and scope, for example, the overall objective of cyber security policy is to manage and control the security performance and strengthen internal security capabilities (Baskerville & Siponen, 2002). The scope of policy is to keep critical information assets safe while reduce the incidences, internal threats and risks (Höne & Eloff, 2002; Lopes & Sá-Soares, 2012). It should be made based on general security principles in specific industry such as Health and Social Care Act (2001), Regulation of Investigatory Powers Act (2000) and so on. This is because company should always comply with these regulations, but the scope of policy must combine with actual business development requirement. Once it is placed, organization should desperately comply with it to enable the enforcement. Practically, content can be enforced by effective security awareness program, education and training, as well as internal audit (Siponen et al, 2009; Moody et al, 2018). The security policy should also be reviewed constantly in order to suit adjustment in management and security development direction (Knapp et al, 2009).

Based on 2011 sub-chapter, the evolving technologies vanishing the traditional working style, companies should make appropriate policy to define the principle of using mobile devices in workplace and after work to prevent data leakage (NIST, 2012; Kaspersky, 2013; Debbie, R, 2002). Besides, cloud computing and social media implemented in business operation requires company to strictly classify their data as "public" "confidential" and "high confidential" in order to be clear what information can be shared on those platforms without harming the security (Kaufman, 2009; Ali et al, 2007). Meanwhile, people who use social media or own devices in the work should strictly follow company data security policy to decrease the internal threats possibility.

5.3 Organization of information security

The objective of management is to ensure the implementation of security policy and program within organization (Dhillon & Backhouse, 2000). Based on IEC/ISO 27002, organization of security consist of internal and external structure; internal structure defines the general scope, responsibilities, procedure and governance, and the external structure consist of different external parties which may access organization's information and system but required to have risk assessment by organization to determine the security implication and control implementation.

Through the review, it has been found that coordination, responsibilities and reporting in internal part, and third-party management in external part have been addressed mostly.

For internal structure, information security issues should be solved by coordination of different parties based on their roles and functions. In 2010, it has been found that there are many security challenges in establishing global coordinative infrastructure since legacy system and different interfaces may result difficulties in consistent authentication; and versatile legal requirements applied to different information platform may create challenges to data protection. As for the responsibilities, board level involvement exists less than expected. Most of investigated companies are still lack sufficient support from board level executives. As to the communication, few of organizations have very matured security communication platform where incidences are properly reported and escalated to critical groups.

To improve this situation, organization should introduce the leadership and build company-wide measures so that all the functions knows the idea from management level and establish information security structure based on that specific focus. This also facilitates constructing consistent global information sharing platform. Besides, board members should prepare proactively to the cyberattacks and put the topic in board agenda since all types of company can become victim today. As for communication, it should not only happen when cyber issues occurred, all the parties should constant communicate on regular basis about security issues to help them to avoid similar problems and cases. To react efficiently to the cyber breaches, company should develop a communication plan and practice with crisis team to improve the feasibility and effectiveness.

In external part, third-party management plays important role in securing company’s information while facilitating its business. The risks associated with introducing third party should be identified and controlled before collaborating with them. Meanwhile, security audit and measures should also be carried out during the cooperation to avoid the breaches risks from outside.

5.4 Human resource security

There is never enough emphasis about human resources in cyber security since human factor is the weakest part in security management. Given the fact that most of cyberattacks were resulted by people who either do not have adequate knowledge about cyber security or with intention of hack, company should constantly train and educate their employees while measure their security performance during prior-employment-termination period.

Based on IEC/ISO 27002, before employment, company should ensure employee, or third party understand their responsibilities in protecting sensitive information. All candidates’ profile should be screened in order to check the conditions for hiring them. Candidate should also sign contract with company for keep save of critical information assets. Third party should implement both technical and administrative control when accessing company's information system. During employment, employee or third party should be aware of their responsibilities in protecting company's information security and equip with updated knowledge to support security performance. Organization should keep training their employees in order to reduce the risks caused by human factors. In the termination phase, employees or third party should return all equipment, information and access back to the organization.

Through the review, we found some obstacles in information security human resources. Both 2013 and 2016 have addressed the insufficient in-house security professionals. Also, by end of 2017, organizations may have up to two million unfilled cyber security positions according to McAfee. On the other hand, fresh graduates have lack of consistency and capabilities for industrial security positions since cyber security is developing all the time. Thus, it requires student to growing their knowledge and skills to face the evolving challenges. This obstacle is also related to company's investment in human resources and training for future talents.

Another problem in organization's information security is inside threats. Nearly all the years reports have addressed the inside threats issues, when comparing to external risks, as higher factor of cyberattack. Besides techniques, most of inside threats are associated with human factors. Year 2016, 2015 and 2008 have revealed that the insider may use his or her access to harm organizational security through unauthorized disclosure, data modification, espionage or other related actions, which will result the loss or damage of company's resources, capabilities, business operation and customer loyalty. However, spotting them is very difficult compared to external risks since they associate with different reasons such as organizational control and monitor, human behavior, financial incentives from outside criminal groups, business competitions, personal hobby and so on.

The third obstacle is security training. Although most of companies realized the importance of it but in practice there are some problems for example who lead the training program and which level of security understanding he or she should have in order to be qualified. In addition, the training content and training effectiveness are hard to be decided and measured (McIlwraith, 2006).

As for the improvement for in-sufficient security experts, industry should gather a wide pool of students and train them as qualified security professionals to meet business requirements (Paulsen et al, 2012). Meanwhile, school education should align practices to evolving security landscape to improve student abilities and skills (Rezgui & Marks, 2008). As for the internal threats, companies should follow IEC/ISO 27002 standard human security part as well as control and manage risks from prior employment to termination (Klein & Luciano, 2016; Siponen et al, 2014). To achieve effective security training, organization should get board level involvement by presenting them costs for cyber security training versus costs for recovery from cyberattack (McFadzean et al, 2007). In case of executive buy-in, enterprise should analyze what is the weakest part of their current systems and how much employees understand the security issues. For example, employees may set up different passwords for systems without awareness of phishing and scam emails which often occurred in their daily works. Meanwhile, training program should be carried out more often than once a year, and team members should help each other to learn and grow their expertise from personal experience or real cases.

5.5 Communication and operational management

This part focuses on establishing communication and operation procedure for managing information security issues within organizations. Since information systems are processing large quantities of organization's information, these systems such as computers, network~~,~~ and mobile devices should be managed in a way that information protection is efficiently facilitated in all business operations. Therefore, meeting this goal requires a clearly defined procedure, responsibilities, strategic plan and measurement in operational management. IEC/ISO 27002 has defined procedures for third party service delivery management, new information system implementation, protection against malicious and mobile code, network security management, media handling, exchange of information and electronic commerce. Among these, network security management has received great attention since network information exchange become popular in todays' internet-based business.

Network information security refers to protecting information transferring between different networks and platforms (Cisco.com-What is network security?). As mentioned in 2015 and 2009 review, social networking sites are primary tool for exchanging information nowadays. In the business, social network can enable the direct communication with customers and end users and this helps company to obtain feedback efficiently and solve customer problems in timely manner (Kaplan & Haenlein, 2009). However, a large amount of information exposed to social network creates cyber risks for companies and enable cyber criminals to target on company's information assets. For example, attackers may hack company's account on social network and send phishing emails to customer which include malware. Obviously, customers will be hacked by malware and it turns out that company will suffer huge trust loss from its customers.

The components of network security include network controls and security of network services (ISO/IEC 27002). Network controls means that network should be controlled and managed adequately to avoid data corruption, manipulation and interception. Security of network service means that company should understand and obligate to security policy offered by network services, and on the other hand monitor the security level of the service to avoid data breach.

In 2015 review, IoT has been address widely by industrial security professionals. This is a network that consists of mobile devices, home application and all kinds of physical devices that can use internet, connection, software and sensors to exchange data. As an emerging technology, IoT has accelerated the connection of devices and enabled convenient access of information; however, unsecured objects have been growing more and more with a greater exposure of risk and potential to be attacked in this network (Weber, 2010). Considering this fact, it is necessary to establish a security mechanism throughout the ecosystem to mitigate the increased risk in devices connection. For example, some basic mechanism such as encryption, firewall, double-level password and advanced mechanism such as cryptographic algorithms should be placed.

As for social network security, 2009 review mentioned that people that are in charge of operating social network should be very careful about the information posted online toward public. One should be equipped with high sense of risk exposure and adequate knowledge to identify the threats from others. Meanwhile, company should constantly monitor the security level of social network and act before being attacked.

5.6 Access control

Access control is vital for business security because it provides gateway for authorized parties while prevent the unauthorized access to internal information (Sandhu & Samarati, 1994). Based on ISO/IEC 27002, access control includes business requirement for access control, user access management, network access control, operating system access control, application and mobile computing access control. The first one means that management should define the access control to information. For example, management should define, develop and publish access control policy which meets business requirements. The key things to consider is who has defined the access control and does the access control support business by its scope? Has the access control been reviewed and updated? What is the process to define access control? The user access management is corresponding to C-I-A triad, so, the use of information and user of information facilities should be authorized by the management in accordance with access control policy. For example, who is eligible to use information facilities and what are the key things to perform when accessing information facilities, such as setting up advanced password, log out when left the services, clear desk and clear screen. The network access control defines user behavior when using network services. For example, organization may not allow anyone to connect network services remotely. The operating system access control defines the authority for using core business functions applications. It requires specialized procedure for using operating system for example, log in procedure, user identification, password management and time out session. The mobile and application access control specifically defines the management of using other services that support the core functions. Key things to consider are: Does the organization allow employees to use mobile devices to save and transfer organization information? Does organization allow remote access to organization information through mobile applications?

Through the review, access control has been addressed by nearly all the years' report. Generally, the discussion can be separated to technical control and non-technical control. As for technical control, 2014 pointed out that only half of the investigated companies have implemented strong technical control to prevent cyberattacks. Meanwhile, when partnering with third party, organizations have not implemented the technical control to limit access from outside and require third party to have remote access limitation. As we know the threats to organization can only be successful when the vulnerabilities are exploited, so technical control in system communications and configuration should be strong enough to safeguard the gateway away from unauthorized access. For non-technical control, basically administrative control, user responsibilities play significant role in the security safeguard process (Colwill, 2009). In the management level, for example Information Security Officer should work in focal point for security compliance and security performance instead of maintaining and developing budget. In the general employee level, organizational security policy should be understood well and implement in daily routine such as no password sharing, table clean and so on.

In general, since people are still the main reason of resulting security issues, organization should give all necessary resources to strengthen this part to decrease the internal risks.

5.7 Incidence management and business continuity

Cyber security incidence management means a process of identifying, managing, recording and analyzing cyber security incidence or threats (Wikipedia.com-Computer Security Incidence Management). The objective of this process is to ensure organization to be equipped with strong capability to manage security events in a timely manner and prevent huge damages to organization (ISO/IEC 27002). According to ISO/IEC 27002, incidence management generally includes two main parts, incidence response and management of incidence response and improvement. As cyber security events continue to grow in volume and complexity, organizations need to apply a series of practices to strengthen their capabilities in rapid identification, response and analysis to mitigate the incidence while become more resilient in the future. The following part briefly introduces these two main parts.

Incidence response includes identifying and reporting security risks, defining investigation and analysis objectives, take proper actions and recovery of system data and information (ISO/IEC 27002). For many organizations, the most critical part is to identify and assess cyber security incidence, whether it has happened and what is the type, damage and extent (Munteanu, 2006). When reporting security breaches, the process should go through appropriate management channel as quick as possible (ISO/IEC 27002). A point of contact should be established for reporting. Correct behavior should be undertaken when information security event happened, for example reporting all-important details, contacting correct person instead of taking own personal reaction to it. The second step is to investigate the situation in a proper manner. Organization should form a professional team to understand as much as possible about the incidence with questions such as: Who has attacked us? What is the purpose of this attack? How long it continues? How much damage we have suffered from the attack? Why we didn't detect this in advance? What are our vulnerabilities in terms of incidence detection and measurement? What proper action organization should take for recovering data and information from cyberattacks? Undertaken action depends on different cases, for example isolating the damaged system with others and blocking all unauthorized access. It is also necessary to check security insurance and report and claim the influence. Generally, the whole process of responding cyber security incidence should be well constructed to prevent disorder in situation.

It is also important to learn after every breach and constantly improve the process. Management of incidence response ensures that responsibilities and procedures are in place in order to efficiently manage the cyber events and report the weakness once it has been found. As to the responsibilities, organization should choose right person who has adequate knowledge in cyber security field to response firstly to the incidence. He or she must identify quickly if any applications need to be involved in the investigation and if organization has the right resources. Meanwhile, incidence management people should constantly learn beyond the current situation in order to prepare for potential upcoming events. As to the procedure, it should be monitored, adjusted and improved with the purpose of efficiently combat with cyber security breaches. Besides, due to sophistication of security issues, procedure should be flexible and developed based on different cases such as information leakage, information system failure, malicious attack. Generally, incidence response should be developed within the scope of management, and people responsible for this procedure should understand clearly the priorities in organization when encountering information security attack.

Through the review, it is obvious that many companies have not yet fully prepared for cyber security incidence. In both 2013 and 2014, companies have experienced different cyberattacks but only few of them have confidence on their incidence response capabilities. There are many reasons may explain this situation. First, small companies have very limited human and technical resources (Atreyi et al, 2003). They often think they are not the targets of cyberattacks so there are no resources and plan prepared for it. Secondly, some companies have conducted the plan and structure for cyber incidence but never really faced the real attack, which leads to the degradation of incidence response management. Thirdly, everything is written on paper but never developed thoroughly in the company. Today many malicious attacks happen in "front-line" employees who may have less adequate knowledge about cyber breaches than higher level executives. They may have insufficient training on how to securely behave and react when cyber breaches happen, which results to bad performance on incidence response. Last, incidence response often includes many details in practice, for example, establishing threats intelligence may not applicable for small business. It is hard for them to obtain a big picture and arrange proper resources accordingly.

Because of above reasons, incidence response can be improved particularly for SMEs from below perspectives. As mentioned above, since incidence management is a large-scale project, which needs time, resources and effort, companies must avoid desiring for everything in the beginning. They should draw a map on current cyber security situation and understand what is the company's critical information that might be "valuable" for outsiders (Wheeler, 2011). Secondly, based on the value of data, they should decide if any tools or workforce is needed for building incidence response management. In most of cases, SMEs should have at least one technician to exam and update the system regularly, and one decision maker to decide if incidence happened and what should be done next. Thirdly, organization should constantly train their employees about backing up data, building safe and strong password to protect the data, preventing malware and phishing software or emails and keep all the smartphones away from unsafety use.

Generally, incidence management is rather a multi-angle project than linear process. It starts with preparation phase and ends with recovery. However, the most important part is to improve the process and prepare for the future incidence. During this cycle, threat intelligence, human and technical resources plays critical importance.

As for the business continuity management, the purpose of it is to minimize the impact from cyber security event to organization and recover the loss of data and information assets (Järveläinen, 2012). It is required to involve information security into the business continuity plan since the consequence of disasters, loss of information and business availabilities will impact business tremendously (Virginia & Michael, 2006). Through the review, 2012 emphasized about this integrated strategy. It has mentioned that the increase of business information sharing, and external communication have led to the increase of authorized access to company's critical information. Therefore, it is essential to implement an integrated security strategy together with business continuity management to fulfill the need of protecting information in different business functions.

5.8 Compliance

Compliance with legal requirements and relevant cyber security regulations can enable company to design and implement its own information security program on standard and qualified level (Burcu et al, 2010). However, compliance does not guarantee the long-term effectiveness of cyber security system; in fact, company should constantly measure the security performance and strengthen the security program to meet the regulations.

The compliance generally includes identification of applicable guidelines, compliance with security regulations and standards, data protection and privacy, technical compliance and information system audit control.

The first step is to understand the regulations and choose the appropriate ones for building and controlling internal information security management. This requires a person or team who can ascertain the requirements and define whether they are determining factors for current situation or for outside vendors. According to IEC/ISO 27002, "all relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization". Besides, the personnel signed with responsibilities should ensure that the organizations meet those requirements by constantly checking the progress. When complying with security regulations and standards, organization should always measure and update the environment it lives in to understand the changes and adjust the requirements. Data protection and privacy policy should be developed in organization and involve all persons who are responsible for privacy information issues. These people should construct the management by giving the guidelines to managers, users and third-party service providers about their responsibilities and duties in managing personal privacy information. It is known that some countries have defined legislation in this area, for example, the Personal Data Act governs the processing of individual personal data in Finland, The Data Protection Act (generated in 1978 and revised in 2004) is the main law that controls the data privacy in France. Company should check and follow these laws when processing the identical information. The technical compliance means that information system should be regularly checked and updated to secure the information in process. The checking shall be executed by experienced professional test engineers with assisting tools, and she or he should generate the compliance checking report. This process should also be executed by authorized person who can access hardware or software under control by management. The compliance checking may also include the penetration test or vulnerability assessment for measuring effectiveness of current controls and system vulnerabilities. Last, information system audit control means that there should be some requirements in place when checking and auditing information system in order to minimize the risks of disruption for business. For example, information system checking should have limited and clear scope, and there should be requirement that identify the resources for performing checking.

Through the review, one can see that data privacy remains problem in many years. In 2009, many companies have clearly understood the privacy policy that has impact on their business, and many have constructed the privacy policy for outside partners. However, only few of them have considered the whole privacy data lifecycle or assessed and monitored the privacy related concerns. On the other hand, users have provided their privacy information for these company without knowing how they deal with it and who else they share this information. Until today, we still see an explosion of privacy crisis occurred in a global social media organization. Although technology strengthen the protection of personal information, the weakest part lies in company's privacy management (Belanger & Crossler, 2011). How to define and protect customer privacy data become a critical process of gaining trust and user loyalty in the market.

As for the compliance with security regulations, 2010 review present a positive picture that almost all the companies have listed the security compliance in organizations top-initiatives. However, in 2012 review, the security control on mobile devices usage seems less effective. Meanwhile, the security regulation compliance performance has not been measured regularly. As mentioned above, company should check the compliance performance in order to improve the management results (Sommestad & Lundholm, 2014). For instance, if company is complying with ISO 27002, it can define measurement level as: 0. incomplete, 1. performed, 2. managed, 3. established, 4. predictable 5. optimized to check if the security policy is in place, whether it has documented and address all areas and if each member of organization knows about those and are complying with those.

As for the audit control, 2013 review emphasized that continuous and proactive assessment of information system helps to identify the "hole" and fix it before cyberattack happen. Besides, an effective audit plan will significantly help the company to identify the potential security risks and consequently avoid or decrease the damage from inside (Kayworth & Whitten, 2010; Cheryl & Rossouw, 2004).

6 Conclusion

Digitalized world is creating huge benefits for innovation, business, technology, government and individuals. With the evolving new products, new markets and new type of consumers, organizations are desperately looking for connections between these to share the benefits of digitalization. In this rush, many companies have not yet fully prepared for risks brought by new wave. The way they embrace the cyber security issues from digitalization defines how they survive in new information age.

This thesis has provided an extensive review on global enterprises cyber security performance from 2008 to 2016 and summarized the most vulnerable pars in information security management based on ISO/IEC 27002. Through the review, one can see fast development and improvement of organizations' internal information security infrastructure; on the one hand, most of information businesses have formalized process to manage information security issues and events, on the other hand, security is no longer the concern of IT department but all functions. To elevate the standing, companies should continue to enhance their security program especially on critical sections and improve security capabilities to react to arising cyber risks and defend cyberattacks.

This study filled the gap between existing knowledge of organizational security practices and suggestions for further improvement. It also gives a benchmark for companies to quickly check their practices in critical parts and improve the situation with specific focus. In general, the study is valuable for studying cyber security development progress among enterprises worldwide during past 9 years, it highlights the changes in cyber security landscape and presents how companies have been reacting to these changes while growing and adapting new possibilities and challenges in digitalized world.

6.1 Limitations

Due to the tight schedule, the extensive review has only extracted figures until 2016. It is important to understand that changes are happening in cyber security landscape every day and situation in different companies' practices also varies. However, the common vulnerable practice found by this research. During 2008 to 2016 still works significant in a way that companies can leverage this information to strengthen their cyber security practice with specific focus. As one can understand this is important for those who have limited budget and resources for information security. Secondly, there are relatively small amount of cyber security survey report made in global scale, which created limitation to present the worldwide picture from main industry in different countries. However, as one can see most of existing global surveys have included sample over 500 respondents, and nearly all respondents were from high-level positions such as ICO, ISO and related function's directors, the quality of data is high enough to serve the intent of study.

6.2 Future research

Nowadays, IoT become a trending topic for many industries. It is also a serious topic from information security perspective since connected devices creates large potential to cyberattacks. Therefore, it is significant to study the potential risks related to IoT when developing network devices for different scenarios combined with previously discovered vulnerability in both administrative and technical parts. Besides, as the new technology arise, manufacturers, businesses and end users are rushing into new things without consideration of security, it is worth to find out bad factors in each sector so that the benefits of IoT can be leveraged at maximum.

REFERENCES

(ISC)2 (2012). ISC2 Global Information Security Workforce Study. pp 6-9

AICPA (2013). The Top 5 Cybercrimes. pp 11, 12, 5

Albrechtsen, E., & Hovden, J. (2010). "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study". Computers & Security, 29(4), pp 432-445

Ali, B., Villegas, W. & Maheswaran, M (2007) "A trust based approach for protecting user data in social networks", CASCON '07 Proceedings of the 2007 conference of the center for advanced studies on Collaborative research, pp 288-293

Anderson, J, M. Why we need a new definition of information security. Computers & Security, 22(4), pp 308

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) Measuring the cost of cybercrime.

Are, N., (2007) "Managing Information Security in Organizations. A case study".

Ashish Garg, Jeffrey Curtis, Hilary Halper, (2003) "Quantifying the financial impact of IT security breaches", Information Management & Computer Security, Vol. 11 Issue: 2, pp.74-83

Atreyi, K., Hock-H, T., Bernard, C, Y, T., & Kwok-K, W., (2003), "An integrative study of information systems security effectiveness", International Journal of Information Management 23, pp. 139–154

Baer, S, W. & Parkinson, A (2007) "Cyber insurance in IT security management". IEEE Security & Privacy, Volume: 5, Issue: 3

Basie, v, S. (2005), "Information Security Governance -Compliance management vs operational management", Computers & Security, Volume 24, Issue 6, Pages 443-447

Belanger, F., & Crossler, R, E (2011) "Privacy in the digital age: a review of information privacy research in information systems", MIS Quarterly, Volume 35 Issue 4, Pages 1017-1042

BERR (2008). Information Security Breaches Survey: Technical Report. pp 23

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). "Information security and risk management". Communications of the ACM, 51(4), pp 64-68.

Brown RB,. (2006). Doing Your Dissertation in Business and Management: The Reality of Research and Writing. Sage Publications

Brynjolfsson & Hitt (2000) "Beyond Computation: Information Technology, Organizational Transformation and Business Performance", Journal of economic perspectives, vol. 14, no. 4, pp. 23-48

Burcu, B., Hasan, C. & Izak, B. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Quarterly, Vol. 34 No. 3 pp 523-548

Chaffey, D. and White, G. (2010) “Business information management: Improving performance using information systems”. Second. UK: Pearson Education.

Chang, S. E., & Lin, C. (2007). “Exploring organizational culture for information security management”, Industrial Management & Data Systems, 107(3), 438-458

Cheryl, V., & Rossouw, v, S. (2004), “Towards information security behavioural compliance”, Computers & Security, Volume 23, Issue 3, pp 191-198

Christopher, J, A., & Audrey, D. (2002), “Managing Information Security Risks: The Octave Approach”. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 2002, ISBN:0321118863.

Cisco (2008). Annual Security Reports. pp 13-14

Cisco (2009). Midyear Security Review, pp 21-22

Cisco (2010). Annual Security Report. pp 6, 10, 12, 17

Cisco.com- What is network security? https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Colwill, C (2009) “Human factors in information security: The insider threat – Who can you trust these days?”, Information Security Technical Report, Volume 14, Issue 4, pp 186-196

Cooper, H. M. (1982). Scientific guidelines for conducting integrative research reviews. Review of Educational Research, 52(2), pp 291-302

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. Knowledge in Society, 1(1), pp. 104-126

CSI (2008). 2008 Internet Crime Report, pp 13-15

CSI (2010/2011). Computer Crime and Security Survey. pp 20

CSI/FBI (2013). Internet Crime Report. pp 3

David Lacey, (2010), "Understanding and transforming organizational security culture", Information Management & Computer Security, Vol. 18 Issue: 1, pp 4-13

Deb, B., Steve, B., Jenn, F. & Rich, G. (2010). A components of MITRE’s Cyber Prep Methodology. Cyber Security Governace. pp 10-11

Debbie, R (2013) “Creating a Mobile-security Policy for Your Organization”, Creative Interactive Ideas

Dell (2016). IBM X-Force Threat Intelligence Index 2017: The year of the mega breach. pp 20

Deloite (2009). Losing Ground 2009 TMT Global Securtiy Survey Key Findings. pp 6-7

Deloitte & Touche (2003). Global Security Survey of the Global Financial Services Industry

Deloitte (2010). Financial Services Global Security Study: the faceless threat. pp 31

Dhillon, G., & Backhouse, J (2000) “Technical opinion: Information system security management in the new millennium”, Communications of the ACM CACM Homepage archive, Volume 43 Issue 7, pp 125-128

Dhillon, G., and Backhouse, J. (2001) "Current directions in IS security research: towards socio-organizational perspectives," Information Systems Journal 11:2, pp. 127-153.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). "The information security policy unpacked: A critical study of the content of university policies". International Journal of Information Management, 29(6), pp 449-457

Dojkovski, S., Lichtenstein, S., & Warren, J, M (2010) "Enabling Information Security Culture: Influences and Challenges for Australian SMEs", in ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems, ACIS, Brisbane

Donnet, B., Gueye, B., & Kaafar, M. A. (2010). A survey on network coordinates systems, design, and security. IEEE Communications Surveys and Tutorials, 12(4), pp 1-2

Donnet, B., Gueye, B., & Kaafar, M. A. (2010). A survey on network coordinates systems, design, and security. IEEE Communications Surveys and Tutorials, 12(4), 488-503.

E&Y (2008). Moving Beyond Compliance: Ernst & Young's 2008 Global Informayion Security Survey. pp 16, 8, 11, 12

E&Y (2010). Borderless security: Ernst & Young's 2010 Global Information Security Survey. pp 4, 7, 13

E&Y (2011). Into the Cloud, out of the fog: Ernst & Young's 2011 Global Information Security Survey. pp 26, 3, 7, 18, 10, 12, 26, 18

E&Y (2012). Fighting to Close the Gap: Key findings from EY's Global Information Security Survey 2012. pp 3, 4, 6, 12, 7

E&Y (2013). Under Cyber Attack: EY'S Global Information Security Survey 2013. pp 6-8

E&Y (2014). Get Ahead of Cyber Crime: EY's Global Information Security Survey 2014. pp 4

Edward, H. (2008) "Information security management standards: Compliance, governance and risk management", Information Security Technical Report, Volume 13, Issue 4, pp 247-255

Eloff, M & Solms, V. (2000). Information Security: Process Evaluation and Product Evaluation

ENISA (2009). Spam Survey – the Fight Against Spam. pp 4

EY (2009). Outpacing change: Ernst & Young's 12th annual global information security survey. pp 3,9, 12

Finra (2015). Report on Cyber Security Practices. pp 4

FraudWatch International (2016). Insights from APWG's 1st Quarter 2016. pp 3

Freitas, S., & Levene, M. (2004). An investigation of the use of simulations and video gaming for supporting exploratory learning and developing higher-order cognitive skills. In Proceedings of the IADIS Cognition and Exploratory Learning in the Digital Age

Gall, M. D., Gall, J. P., & Borg, W. R. (2007) Educational research: An introduction. Boston: Pearson Education.

Gartner.com. Identify and Access Management (IAM) https://www.gartner.com/it-glossary/identity-and-access-management-iam/

Gregory, D, M., and Mikko, S., & Sepoo, P (2018) "Toward a unified model of information security policy compliance", MIS Quarterly Vol. 42, pp. 1-27

Guidelines for Managing and Securing Mobile Devices in the Enterprise, NIST SP 800–124, 2012.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). "Implementation and effectiveness of organizational information security measures". Information Management & Computer Security, 16(4), pp 377-397.

Hart, C. (1999). Doing a literature review: Releasing the social science research imagination. pp 3-16

Harvey, M. (2010). 05-771: What is Literature Review. pp 1-2

Heather, F. & Neil, F, D., (2003), "The application of information security policies in large UK-based organizations: an exploratory investigation", Information Management & Computer Security, Vol. 11 Issue: 3, pp.106-114

Henderson, J, C., & Venkatraman, H (1999) "Strategic alignment: Leveraging information technology for transforming organizations", IBM Systems Journal, Volume 38, Issue 2.3, pp 472-484

HIMSS (2013). 6th Annual HIMSS Security Survey. pp 4-5

Höne, K & Eloff, J, H, P (2002) "Information Security Policy: What do International Information Security Standards Say?", ISSA 2002 2nd Annual Conference, Mistry Hills

Huseyin, C & Srinivasan, R & Wei, Y (2008). Decision-theoretic and Game-Theoretic Approach to IT Security Investment. Journal of Management Information Systems Volume 25 Issue 2. pp 282

IBM & Ponemon (2016). 2016 Cost of Data Breach Survey. pp 2-3

IBM (2017). IBM X-Force Threat intelligence 2017. pp 3-4, 5, 6

InfoSecurity & PwC (2010). Information Security Breaches Survey: technical support. pp 2-3, 4-7, 9

ISACA (2014). State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey. pp 20

ISO/IEC 27002. Information technology-Security Techniques-Code of practice for information security management

IT Governance Institute (2010). Information Security Governance: guidelines for boards of directors and executive management. pp 17

IT Outsourcing Security (2008). The Government of the Hong Kong Special Administrative Region. pp 7

Janine, L, Spears. & Henri, B., (2010), "User Participation in Information Systems Security Risk Management", Mis Quarterly, Vol. 34, No. 3, pp. 503-522

Janne, M, H., Eirik, A., & Jan, H., (2008), "Implementation and effectiveness of organizational information security measures", Information Management & Computer Security, Vol. 16 Issue: 4, pp.377-397

Järveläinen, J (2012) "Information security and business continuity management in interorganizational IT relationships", Information Management & Computer Security, Vol. 20 Issue: 5, pp.332-349

Jesson, J., Matheson, L., & Lacey, F. M. (2011). Doing your literature review: Traditional and systematic techniques.

John, D., Anat, H & Dennis, G., (2009), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", Information System Research, Volume 20, Issue 1, pp. 1-157

Joo, S, Lim., and Shanton, C., & Sean, M., & Atif, A (2009) "Exploring the Relationship between Organizational Culture and Information Security Culture", the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia

Kaplan A, M., Haenlein, M (2009) "Users of the world, unite! The challenges and opportunities of Social Media", Business Horizons, 53, pp 59-68

Kaspersky (2012). Global IT Security Risks: 2012. pp 2

Kaspersky Lab (2013) "Global Corporate IT Security Risks: 2013"

Kaufman, M, L (2009) "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Volume: 7, Issue: 4, pp 61-64

Kayworth, T. & Whitten, D (2012) "Effective Information Security Requires a Balance of Social and Technology Factors", MIS Quarterly Executive, Vol. 9, No. 3

Kenneth J. K., Thomas E. M., R, Kelly, R, Jr., & Dorsey, W, M. (2006). The top information security issues facing organizations: what can government do to help? Information Secuity and Rrisk Management, pp 51-58.

Kenneth, J., Knapp, T, E., Marshall, R., Kelly R, F., & Nelson, F. (2006), "Information security: management's effect on culture and policy", Information Management & Computer Security, Vol. 14 Issue: 1, pp.24-36

Kerry-L, T., Rossouw, v, S., & Lynette, L. (2006), "Cultivating an organizational information security culture", Computer Fraud & Security

KJ, Spike Q (2010). New Zealand Computer Crime and Security Survey. pp 12

Klein, R, H., & Luciano, E, M. (2016) "What influences information security be behavior? a study with brazilian users", JISTEM - Journal of Information Systems and Technology Management, Vol. 13, No. 3, pp. 479-496

Knapp, J, K., Morris Jr., R, Franklin, Marshall, E, T., & Byrd, T, A. (2009) "Information security policy: An organizational-level process model", Computers & Security, Volume 28, Issue 7, pp 493-508

Kruger, H, A., & Kearney, W, D. (2006), "A prototype for assessing information security awareness", Computers & Security, Volume 25, Issue 4, pp 289-296

Kuyoro, S, O., Ibikunle, F., & Awodele, O (2011) "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume 3, Issue 5, pp 247-255

Kwo-Shing Hong, Yen-Ping Chi, Louis R. Chao, Jih-Hsing Tang, (2003) "An integrated system theory of information security management", Information Management & Computer Security, Vol. 11 Issue: 5, pp.243-248

L.A. Gordon & M.P. Leob (2002). The economics of Investment in Information Secuity. -ACM Transactions on Inforation and System Security.

Landoll, J, D., & Landoll, D (2005). “The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments”, Taylor & Francis Group, Boca Raton

Lawrence, A. G., Loeb, M. P. & Tashfeen, S (2008). “A framework for using insurance for cyber-risk management”. Communications of the acm, vol. 46, No. 3

Levy, Y., & Ellis, T. J. (2006a). A systems approach to conduct an effective literature review in support of information systems research. Informing Science: International Journal of an Emerging Transdiscipline, 9, 181-212.

Lopes, M, I & Sá-Soares, d, Filipe (2012) “Information Security Policies: A Content Analysis”, PACIS 2012 Proceedings, pp 146.

Lu, Y & Ramanurthy (2011) “Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination”, MIS Quarterly, Vol. 35, No. 4, pp. 931-954

Martin N, Rice, J. (1997) “Cybercrime: understanding and addressing the concerns of stakeholders”. Computers & Security, 30: 803-14.

Mathieu, T. & Guy, P. (2015). A Framework for Guiding and Evaluating Literature reviews. Communications of the Association for Information System, 37(6), pp 6

McFadzean, E., Ezingeard, J, N & Birchall, D. (2007) "Perception of risk and the strategic impact of existing IT on information security strategy at board level", Online Information Review, Vol. 31 Issue: 5, pp.622-660

McIlwraith, A (2006). “Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness”. Gower Publishing Company.

Melville, N., Kraemer, K., & Gurbaxani, V (2004) “Review: information technology and organizational performance: an integrative model of it business value”, MIS Quarterly, Volume 28 Issue 2, pp 283-322

Merrill, W. & Rober, W., (2009), “Behavioral and policy issues in information systems security: the insider threat”, European Journal of Information Systems, 18, pp. 101– 105

Munteanu, A. (2006) “Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma”, Managing Information in the Digital Economy: Issues& Solutions, pp 227-232

Ng, Z, X., Ahmad, A., & Maynard, B, S (2013) “Information Security Management: Factors that Influence Security Investments in SMES”, Australian Information Security Management Conference, pp 60-74

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Sprouts, 10(26), 1-46.

PandaLabs (2009). Annual Report pp 4, 5, 6

Parker, D.B. (1998) “Fighting computer crime – A new framework for protecting information”, New York

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012) “NICE: Creating a Cybersecurity Workforce and Aware Public”, EEE Security & Privacy, Volume 10, Issue 3, pp 76-79

Perry, W (1985). Management Strategies for Computer Security. USA: Butterworth Publishers. pp 94-95

Perry, W.E. (1985) “Management Strategies for Computer Security”, New York

Ponemon (2010). Perceptions about Network Security: Survey of IT & IT Practitioners in the U.S. pp 21

Ponemon (2016). Cost of Data Breach Study: Global Analysis. pp 2

Ponemon Institute LLC (2014). Critical Infrastructure: Security Preparedness and Maturity. pp 13, 14

Powell, W, C., & Dent-Micallef, A (1999) “Information technology as competitive advantage: the role of human, business, and technology resources”, Strategic Management Journal, Volume18, Issue5, pp 375-405

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778.

PwC (2010). The PwC Global State of Information Security Survey: Some key findings from UK Respondents. pp 6, 3

PwC (2012). Information Security Breaches Survey: Technical report. pp 8

PwC (2014). US cybercrime: Rising risks, reduced readiness: key findings from the 2014 US State of Cybercrime Survey. pp 14

PwC (2016). Turnaround and Transformation in Cybersecurity. Key findings from the Global State of Information Security Survey. pp 3-4, 5-6, 8

PwC (2016). Turnaround and transformation in cybersecutity: Key Findings from the Global State of Information Security Survey 2016. pp 25, 5-6, 8

Qing, H., Paul & Donna, C. (2006), “The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective”, Proceedings of the 39th Hawaii International Conference on System Sciences.

Qing, H., Tamara, D., Paul, H. & Donna, C. (2012), “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture”, Decision Science.

Radicati (2009). Email Statistic Report 2009-2013. pp 4-5

RAS (2010). Global Online Consumer Security Survey. pp 1

Rasmussen, J (1997) “Risk management in a dynamic society: a modelling problem”, Safety Science Volume 27, Issues 2–3, pp 183-213

Raymond, L. (1990), “Organizational context and information systems success: a contingency approach”, Journal of Management Information Systems, Vol. 6 No. 4, pp. 5-20.

Rezgui, Y. & Marks, A (2008) “Information security awareness in higher education: An exploratory study”, Computers & Security, Volume 27, Issues 7–8, pp 241-253

Richard, B & Siponen, M (2002), "An information security meta-policy for emergent organizations", Logistics Information Management, Vol. 15, Issue, 5/6 pp. 337-346

Rok, B. & Borka, J-B. (2008), "An economic modelling approach to information security risk management", International Journal of Information Management, Volume 28, Issue 5, Pages 413-422

Rubenstein, S., & Francis, T. (2008). "Are your medical records at risk?", Wall Street Journal – Eastern Edition, 251(100), D1-D2.

S. Subashini & V. Kavitha (2010). A survey on Security issues in Service Delivery Models of cloud Computing. Journal of Network and Computer Applications. 34 (2011).

Sandhu, R, S., & Samarati, P (1994) "Access control: principle and practice", IEEE Communications Magazine, Volume 32, Issue 9

SANS (2002). An Overview of Threat and Risk Assessment.

SANS (2002). Using security to protect the privacy of customer information. pp 1-2

SANS (2006). An Introduction to Information Security Risk Management. pp 1

SANS (2012). Results of the SANS SCADA Security Survey. pp 5

SANS (2016). IT Security Spending Trends. pp 4-5

SANS (2016). State of Cyber Security Implications for 2016: An ISACA and RSA Conference Survey. pp 8-9, 10

SANS Institude (2007). Information Security Policy-A Development Guide for Large and Small Companies.

Sara, K., Pascale, C., & John, C, (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", Computer & Security, Volume 28, Issue 7, pp. 509-520.

Schweitzer, J.A. (1982) "Managing information security: A program for the electronic information Age", Boston. MA.

SecurityWeek (2013). Adobe Confirms Source Code Breach, Theft of customer Data https://www.securityweek.com/adobe-confirms-source-code-breach-theft-customer-data

Shuchih, E, C., & Chienta, B, H. (2006) "Organizational factors to the effectiveness of implementing information security management", Industrial Management & Data Systems, Vol. 106 Issue: 3, pp.345-361

Shuchih, E, C., & Chin-S, L. (2007), "Exploring organizational culture for information security management", Industrial Management & Data Systems, Vol. 107, Issue: 3, pp. 438-458

Siponen, M (2000), "A Conceptual Foundation for Organizational Information Security awareness", Information Management & Computer Security, 8/1 (2000), 31-41

Siponen, M., & Livari, J (2006) "Six Design Theories for IS Security Policies and Guidelines", Journal of the Association for Information Systems Vol. 7 No. 7, pp. 445-472

Siponen, M., Mahmood, M. A., & and Pahnila, S. (2014). “Employees’ adherence to information security policies: An exploratory field study”. Information & Management, 51(2), pp 217-224.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). “Are employees putting your company at risk by not following information security policies?” Communications of the ACM, 52(12), pp 145-147.

Solms, v, R., & Niekerk, v, J (2013) “From information security to cyber security”, Computers & Security, Volume 38, pp 97-102

Sommestad, T., Hallberg, J., Lundholm, K & Bengtsson, J. (2014) "Variables influencing information security policy compliance: A systematic review of quantitative studies", Information Management & Computer Security, Vol. 22 Issue: 1, pp.42-75,

Stonebruner, G., Goguen, Y, A & Feringa, A. (2002). “SP 800-30. Risk Management Guide for Information Technology Systems”, National Institute of Standards & Technology Gaithersburg, MD, United States

Straub, D. W. 1990. “Effective IS Security: An Empirical Study,” Information Systems Research (1:3), pp. 255-276

Sultan, A, N (2010) “Reaching for the “cloud”: How SMEs can manage”, International Journal of Information Management, Volume 31, Issue 3, pp 272-278

Symantec (2010). SMB Information Protection Survey Global Data. pp 5

Symantec (2013). Internet Security Threat Report. pp 12

Symantec (2016). Internet Security Threat Report. pp 6

Symantec (2016). Internet Security Threat Report. pp 6

Techopedia Data Security: https://www.techopedia.com/definition/26464/data-security

Tipton, H. & Krause, M. (2007) “Information security management handbook”, Boca Raton

Tobias, R., Sean, M., & Shanton, C (2007) “Organizational security culture: Extending the end-user perspective”, Computers & Security, Volume 26, Issue 1, pp 56-62

Trustwave (2014). 2014 Security Pressures Report. pp 2

Unisphere (2014). DBA-Security Superhero: 2014 Ioug enterprise data security survey. pp 3-4

US-CERT. Technical Trends in Phishing Attacks. pp 1-2

Verizon (2008). Data Breach Investigations Report. pp 10, 12

Virginia, C & Michael, J. C (2006) “Business Continuity Planning: A Comprehensive Approach”, Information Systems Management, Volume 21, Issue 3

Warman, A.R. (1992) “Organizational computer security policy: the reality”, European Journal of Information Systems, Vol. 1 No. 5, pp. 305-10

Weber, R, H (2010) “Internet of Things – New security and privacy challenges”, Computer Law & Security Review Volume 26, Issue 1, pp 23-30

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), pp 13–23

Wheeler, E (2011) “Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress Publishing 2011

Whitman, M. E. (2004). “In defense of the realm: Understanding the threats to information security”, International Journal of Information Management, 24(1), 43-57.

Wikipedia, Phishing https://en.wikipedia.org/wiki/Phishing

Wikipedia.com. Lockheed Martin, https://en.wikipedia.org/wiki/Lockheed_Martin

Wikipedia.com-Computer Security Incidence Management, https://en.wikipedia.org/wiki/Computer_security_incident_managemet

Wikipedia: Computer Security Incidence Management https://en.wikipedia.org/wiki/Computer_security_incident_managemet

Yang, S, M., Yang, M, H. & Wu, B. (2005), “The impacts of establishing enterprise information portals on e-business performance”, Industrial Management & Data Systems, Vol. 105 No. 3, pp. 349-368.

Yildirim, E, Y., Akalp, G., Aytac, S., & Bayram, N (2010) “Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey”, International Journal of Information Management, Volume 31, Issue 4, pp 360-365

Zhang, X,m Wuwong, N., Li, H & Zhang, X (2010). “Information Security Risk Management Framework for the Cloud Computing Environments”, 2010 10th IEEE International Conference on Computer and Information Technology, Bradford, UK