Leadership by Example in e-Government Security Management System

Dyana Zainudin
Cardiff Metropolitan University
Cardiff School of Management
Wales, United Kingdom

Thaier Hamid, PhD
Cardiff Metropolitan University
Cardiff School of Management
Wales, United Kingdom

Atta Ur-Rahman, PhD
Cardiff Metropolitan University
Cardiff School of Management
Wales, United Kingdom

ABSTRACT
e-Government is getting advance in targeting efficient services to citizens, hence, information security becomes an important asset to the national entities. Information security maturity level by Von Solms is theoretically has improved from technical to governance wave. However, a problem exists when theory does not align with the current practice because practically, the employees' mind-set is still in technical wave and organisations' strategy partially involve governance wave especially a leadership context. These can also be found by a previous contribution made by Zakaria studies, he describes a leadership stays under the manager's responsibilities. His study is a continuation of a Schein's organisation culture. Schein defines culture with three layers of values, observable and assumption, in additions Zakaria has improvised into security culture becomes security value, observable and assumption. However, manager's responsibilities stay under management wave; meanwhile, governance wave involves top management. Thus, the composition explores a 'leadership-by-example' in e-Government security management system in order to come out with a model of key-factors to line up with governance wave. In order to develop a 'leadership-by-example' concept in the e-Government management system, the authors guide the study with four objectives and are achieved in different sections. The authors concluded an empirical study by critically reviewing previous literatures that are achieved in section 2, and followed by evaluation of leaders' strategy on information security development and its implementation and distribution to employees which described in section 4. Findings from the study show an inappropriate strategy of leadership concept in the organisations creates lack of motivation to employees which can be a cause of incidents by insiders. Inappropriate strategy of leadership concept is due to incompatible security leadership and unorganised security structure. Therefore, the study contributes a model of key-factors contains of 3Ps includes 'People', 'Process' and 'Product' to guide on the concept of 'leadership-by-example' in managing information security management system systematically.

General Terms
Information Security Management System, People & Security and Leadership-by-Example.

Keywords
e-Government, information security, leadership, information security culture, human factor, cyber threats, risk management.

1. INTRODUCTION
The work shows an extensive contribution from previous researches which mostly concentrate on law enforcement, punishments and awards, manager's responsibilities and etc. This study explores on leadership-by-example related to top management level align with governance wave in e-Government security culture. The paper mainly investigates the source-cause factor of vulnerabilities in e-Government security culture which emphasises on leadership and its consequence to human conduct. An aim is filling the gaps of previous researches in order to propose a model of key-factors in securing e-Government.

Essentially, e-Government has become an international agenda for many years. Since 1990s, many governments despite any levels have initiated to enforce e-Government projects in a way to provide electronic information and services to citizens and businesses (Martinez-Moyano, 2007). The e-Government helps to achieve as a better government in terms of services to citizens. Besides a service to citizens, e-Government also operates as an interaction medium between Government-to-Citizen or Government-to-Consumer (G2C), Government-to-Business (G2B), Government-to-Government (G2G) and Government-to-Employees (G2E).

Technology has its own strengths and weaknesses and so does e-Government. e-Government has many benefits such as service efficiency, cost and time effectiveness and convenient to all parties. e-Government also simplifies tasks for all and gives an easier access for every party to communicate. However, a weakness of e-Government service that comes to the authors' concern is security vulnerability. The vulnerability leads to cyber-attacks that will affect economic, social, and political factors. Also, it may impact to the personal privacy leakage, as the government has an easy access to its citizens.

These risks of the translation of the traditional government to electronic government have demonstrated that it has become an important policy decision to every government in the history (Stephen Smith, 2006). e-Government risks and security issues has become as national threats. The aim of e-Government security management system is to offer a guideline to safeguard the national information (Gams, 2000) and most governments nowadays adopt an information protection management system approach.

Thus, in parliamentary procedure to minimise risks, the study comes out with a model of key-factors, but, firstly the authors considered on a related work which is explained the background of study in the next section followed by research methodology in section 3. The section 3 describes the study process and its concept to investigate the relationship between leadership and its effect to employees' behaviour. Then, analysis and discussion of study are shown in section 4 and 5. In section 6, the authors conclude the overall study.

2. BACKGROUND

The paper explains the development of information security as well as the relevant literature on security culture. The study defines that the development of information security management is divided into four waves/phases as according to Von Solms (Von Solms, 2006). There are developments in technical, management, institutionalisation and governance.

Technical is when information security is only in technical perspective, such as, using the security metrics and attack graphs to prevent the harm to the confidentiality, integrity, or availability (CIA) and ultimately cause the degradation of a system, or even make it unusable (Hamid, Thaier, 2014). Then, organisation starts to realise the importance of managing the technical security, therefore, the manager's task was in charge to make sure that the information security is well managed and secure. Nonetheless, there was no guideline in managing information protection. Hence, the massive improvement in the institutionalisation of information security began in 1990s through standardisation, certification and implementation of security metrics to assess information security aspects in organisations. Afterwards that, governance plays its role as an important element in the information security development, especially in legal and regulative demands. The next sub-part is to briefly describe each wave in Von Solms theory.

2.1 Von Solms Theory

1st wave – The wave describes about technological when the problems to be handed-in to technical person who work under the Information Technology (IT) department that mainly accountable for any incidents happen or known as IT technician.

2nd wave – The wave improved from IT technician to management responsibilities. Managers are responsible to manage information security. In this phase, information security policies and procedures were created.

3rd wave – The improvement of the 2nd wave of policies and procedures has turned into standardisation mode. The international best practices and certifications were introduced.

4th wave – The latest wave introduced in 2012 is the governance, development of information security. A governance development includes risk management and top management in order to ensure the availability, integrity, confidentiality and traceability (DICT) of information.

2.2 Governance

The number of organisations depending on information system has kept increasing each year. The revolution of an information system from computer system is now improving to smartphone and tablet applications. The revolution pace keeps improving very quickly. Technology development is growing very fast. According to Gartner, the technology will grow fast, hence, organisations have to deal 30 times more information than what they are facing today with the chaos, security vulnerabilities and risk management etc. (IT Governance Institute, 2006). The situation has made organisation to become a victim and a witness at the same, of growing technology development which create more potential cybercrimes.

The technology development in some ways has burdening organisations, especially a board of directors to overcome the situation and to plan for risk mitigation and to provide an extra financial budget in protecting information. Not like before, organisations can physically secure the room with full of data files inside the room and no extra cost needed. However, nowadays, the growing numbers of cybercrimes have given extra responsibility to the board of director to provide extra cost and extra protection to prevent information assets from affecting the business finances and reputation.

Organisations are mostly focusing on security to protect information system which rather than to protect the information itself. For them, by protecting information system, then all information will be fully protected and safe. This thought has made organisations are fully relying on information technology department responsibilities in protecting the information. This approach is too narrow to completely secure the organisation information. In this approach, board of director will fully have transferred all burdens and responsibilities to the information technology department.

In order to achieve the security effectiveness, information security shall involve the highest level of organisation. Information security is not only about technical, but the whole business processes. Therefore, the approach must be viewed as a big scope of organisations; it takes a lot of work starting from the highest level of small positions in organisations, in a way to mitigate risks, system and network vulnerabilities, the security processes, security knowledge, human resource security, physical security and etc. It involves all departments, especially board of directors and not only information technology department.

2.3 Human Firewall

According to a literature review on organisational culture contributed by Schein's, organisational culture defines as a combination of layers; observable artefacts, values and basic underlying assumptions (Schein, 1992). These are important in defining culture within the organisation's study as it brings a powerful influence that ability to give impacts to employees' behaviour. An appropriate culture encourages employees to perform security practices. It is based on the understanding of instilling organisational culture into information security culture context.

Zakaria has contributed the rationalisation of the relationship between organisational culture and information security which lead to the development and establishment of an information security culture framework (Zakaria, 2007). This has presumed as evidence that an information security culture is developed by the culture within an organisation. Information security culture is activities which support the information security implementation and its effectiveness when its development can change an employees' behaviour (Zakaria, 2007). Information security culture acts as "human firewall" in order to safeguard the organisation's information assets and etc. Hence, the study will create an understanding of 'leadership-by-example' concept as a root-factor of human firewall.

2.4 National Security Dilemma

Nowadays, the national security is not only being threatened by physical. This is a new national security dilemma. According to Oxford scholar, traditional security involves countries and people are not only threatened by interstate wars which is wars between countries or a violent conflict that involves civil wars, ethnic and religious conflicts, cross-border wars, transnational terrorism, and etc. But the modern threats also have dragged into a new security dilemma which involves environment of complex economic interdependence, multiculturalism, and asymmetric power relations within

countries (Cerny, 2010). Based on this, then the authors found within a new national security dilemma, information is part of modern threats to countries, especially on its availability, integrity and confidentiality of national information. Physical threats are based military modes and mechanisms to protect national security. But, a modern high technology creates latest security dilemma for countries in national cyber security threats and risks.

3. METHODOLOGY

The study explores all relevant methodological elements and discussed according to an integration of each element in Schein's organisational culture model and also Zakaria's information security culture model. The same characteristics in conceptual model are used as the study is a continuing study of Schein's and Zakaria's framework.

The adapted model comprises of three levels: surface manifestations, values and basic assumptions. Surface manifestations define the tangible culture observation that is able to see in physically and able to be heard, such as visible products and visible and audible behaviours. Values explain the partially visible aspect in an organisation to understand the behaviour such as security documentations. Basic assumptions describe the indirect behaviour among employee that is not easy to understand by observation method. See Fig 1.

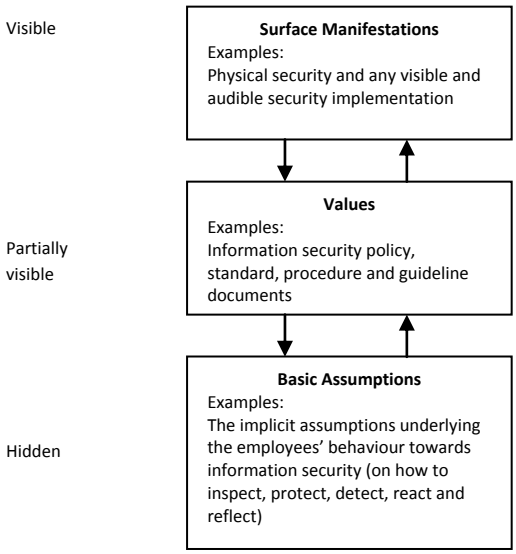

Fig 1 Three level of security culture model (Zakaria, 2007)

The framework is then to determine current leaders' activities and its effect on security culture. In this concept, both surface manifestation and values are not enough to gain an accurate data for the study; therefore, the basic assumption is used to understand security behaviour.

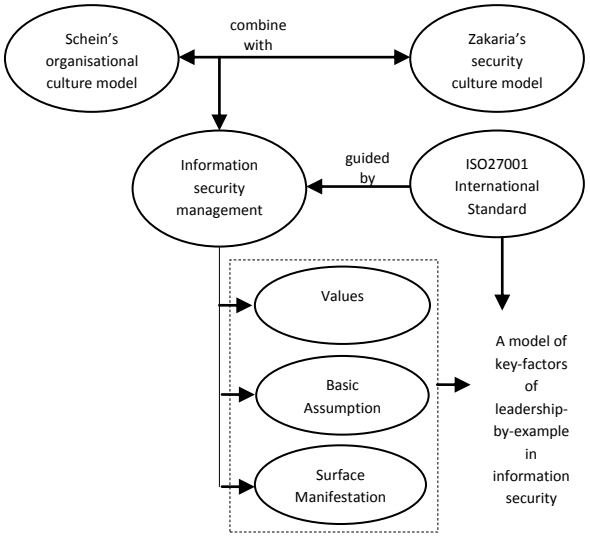

Fig 2 A conceptual model for the study

The first level is a value of the selected government to study on current information security management system in order to understand their security maturity level in managing information security management system. The second level is the basic assumptions to relate to the knowledge that the strategic level has in order to manage the organisation and its effectiveness of employees. The third level is to find out the surface manifestations which are a physical representation control.

Table 1 Research methodology based on levels

Level	Method used
Value	Interview Open-ended questionnaire
Basic assumption	Open-ended questionnaire
Surface manifestation	Observation

Therefore, qualitative method is used for the study. See Table 1. Semi-structured interview and questionnaire are the chosen methods to investigate the value and basic assumption. Meanwhile, observation is used to investigate physical control access. The chosen qualitative research methods enable the study to analyse a social and cultural phenomenon in security behaviour such as assumptions, norms, routine and etc. The study is interested in finding the answers to questions on "how" the leadership works and "why" to the current security practices, assumptions and perceptions.

Table 2 Number of candidates

Method used	Number of candidates
Interview	SL= 6
Open-ended questionnaires	SL= 6; TL= 9; OL+RW=43
Observation	Random

**SL=Strategic Level; TL=Tactical Level; OL=Operational Level; RW=Random Workforce.*

The paper evaluates on leadership practices, capabilities of information security, security strategy, knowledge and awareness. Based on the interview result, then the study continues with in-depth investigation with open-ended questionnaires. Three sets of questionnaires were distributed to four different levels which are strategic, tactical, operational and random workforce level. Only the operational

and random workforce level received the same set of questionnaire. Physical security was observed at any times in the middle of the study. See Table 2.

3.1 Interview

The interview aims to investigate indirect security behaviour to understand how the information security management system is being developed and implemented. The interview holds in an informal and open discussion with the strategic level to see their strategy, their security concerns on employees' behaviour, the way they develop the security documentation and etc. The authors chose to do open discussion in order to receive an honest feedback from the strategic level. The authors believe a formal interview will limit them in giving answers as well as opinion/concerns in an honest and open way. Therefore, the authors chose to make them feel comfortable having an open discussion with the authors. The interview questions are open-ended questions and the respondents' answers are noted down by the authors, then to transfer to the voice recorder for back-up for later transcription.

3.2 Questionnaires

For strategic level, at this stage, the paper continues study on leadership skills as well as their knowledge and awareness on information security protection by preparing further questions to examine their skills. The work also considers their opinion on how they think of their leadership skill in managing information security management system and as considerably as their loyalty. Their opinions on human factors in security breach and as well as leadership-by-example concept in information security management system is also evaluated.

For the tactical level, the paper investigates on their knowledge and awareness about information security and its management system. The intellect is to compare on strategic level feedback on giving training and consciousness to their employees and how the employees have the awareness.

For the operational and random workforce level, the study mostly to measure their knowledge and awareness of information security and the caliber of leadership they took in. For this level, the authors also considering finds out their concerns on information security management system as well as their opinions about leadership-by-example concept.

3.3 Observation

The observational approach enables the authors to gain first-hand experience and a better understanding on in front side of physical access especially among random workforce level. The direct observation didn't interrupt their everyday working activities. The direct observation only involves behaviours, activities and physical objects during the evaluation include physical and environmental security and access control. This approach did not let the participants notice or aware that all their activities were being observed. This is to make sure that the authors gain natural findings without changing their normal behaviour. Thus, the evidence for this observation can help the authors to gain additional information about this investigation.

Therefore, the authors then compare the finding from the observation with collected data from the questionnaires and the interviews in order to identify gaps between official security behaviour, the assumption and the actual security behaviour.

4. ANALYSIS

The paper demonstrates an analysis of the study to all levels. Firstly, the strategic structure of the whole view of selected government's security implementation has too many escalations parties from different agency bodies with different security tasks throughout the whole process of information security.

The strategic level investigation revealed the vulnerabilities of the selected leaders in managing employees, especially in terms of security knowledge and capabilities. Finding also shows information security allocations were located as a sub-division of information technology division. The result also found less structured on security communication for training and awareness to employees. Strategic system in developing an information security management system also involved many parties upon readiness development.

Meanwhile, tactical level study shows the size of organisation affect the security knowledge among employees because not all divisions involve and receive updates about information security. The study on tactical level also found that different departments have different feedback on the frequency of conducting the training and awareness. The result has also found that there were no managers have information security knowledge, even though they are among individual in the information technology division. Meanwhile, almost quarter of the managers say that they are weak in information security implementation, especially those who were from the human resource division.

The study further investigated on questionnaire results for operational and random workforce. These levels are from executive level and below that responsible to implement and comply with information security policies and procedures. The study found the similar cases as in tactical level where the training and awareness is not thoroughly conducted to every division and quarter of them said they do not have awareness posters in their divisions and most of them were from the human resource division.

The study also found that they were lack of knowledge about information security such as awareness of virus protection and also malware prevention through external storage device infection such as USB sticks.

5. DISCUSSION

The gaps fulfil the element of key-factors that resulted as the key-factors model of leadership-by-example in e-Government security services. The paper claims that in order to minimise security risks, the leaders have to focus on their own commitment instead of only providing guidelines to employees. The study demonstrates a correlation commitment between management and employees' that contributes a concept of understanding that leadership is a key element of cyber threat prevention.

The paper proposes 3Ps in improving e-Government services security using leadership-by-example. The 3Ps stands for Process, People and Product. Each key element in this model defines key-factors in developing leadership-by-example. Each element comprises a DeGoSec Model, Norms vs Change and 3Ts Theory.

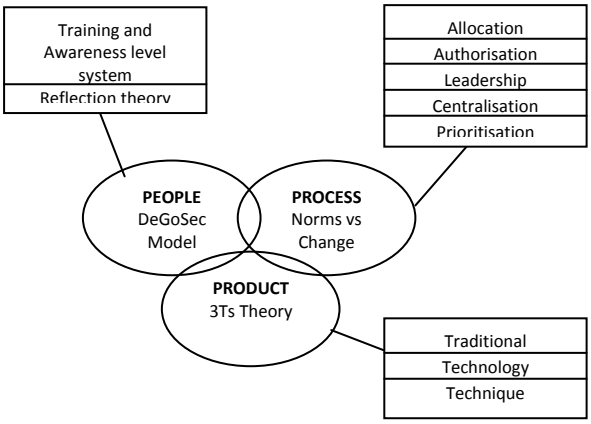

Fig 3 Leadership-by-example key-factors in e-Government security management

5.1 People element

People consists of five aspects which are allocation, authorisation, leadership, centralisation and prioritisation

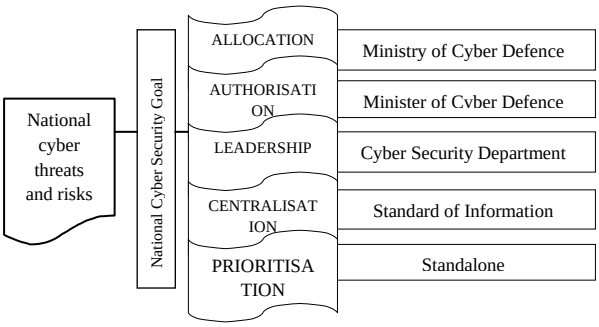

Fig 4 DeGoSec Model

5.1.1 Allocation

The allocation is to designate its own Ministry of Cyber Defence in cabinet members. The Ministry of Cyber Defence functions as to protect the national information from any threats. The allocation is to ensure that the segregation of national defence both physical and information is to be two different aspects. The segregation of these two aspects is to increase the protection of national cyber threats and risks. All agencies that responsibilities for information security are to be allocated in one roof under the Ministry of Cyber Defence that lead by the Minister of Cyber Defence.

5.1.2 Authorisation

Authorisation is to create the aspect of actual rights in making decisions which relates to any matters about national cyber security. The authorisation is suggested by the authors with having its own Minister of Cyber Defence. As to improve the current strategy, structure, the cabinet is suggested to have a representor from the cyber security area in a cabinet meeting in deciding the best result for national cyber security threats and perils. This is to assure that the government is fully regulated. Furthermore, it is to enable an authority for the direct access right to discuss and make decisions with cabinet members without having to go through many layers before reaching to cabinet members, especially in terms of information risk management such as budget allocations, prevention management and incident handlings. In authorisation, the study comes out with the rationalisation of the 7Cs of security knowledge, leadership which are Context, Competence, Culture, Communities, Conversation and Common language, Communication and Coaching. See Table 3.

Table 3 7Cs of security knowledge leadership

Characteristics	Index
1.0 Context	1.0.1 Vision 1.0.2 Passion 1.0.3 Ability 1.0.4 Walk-the-Talk 1.0.5 Convey
2.0 Competence	2.0.1Direction setting 2.0.2 Change Leadership 2.0.3 Critical Thinking 2.0.4 Organisational Development and Diversity 2.0.5 Personal Organisation Balance 2.0.6 Quality 2.0.7 Knowledgeable 2.0.8 Innovative
3.0 Culture	3.0.1 Top-down 3.0.2 Positivity
4.0 Communities	4.0.1 Appreciation
5.0 Conversation and Common Language	5.0.1 Straightforward 5.0.2 Absorbance
6.0 Communication	6.0.1 Reachability 6.0.2 Two-way 6.0.3 Indefinite learn
7.0 Coaching	7.0.1 Oriented 7.0.2 Supportive 7.0.3 Motivation

5.1.3 Leadership

Every ministry shall have an independent Cyber Security Department it guided by the Ministry of Defence. The Ministry of Cyber Defence is to consult Cyber Security Department in every ministry. This includes training and awareness rising. The suggestion is to point out the standard system in every organisation structure to ensure the quality of implementation and practices of information security.

5.1.4 Centralisation

Centralisation is to prevent a decision making made by Minister of Cyber Defence and all departments shall implement information security with the systematic standard guided by the Minister of Cyber Defence. The head of Cyber Security Departments will refer to the Minister of Cyber Defence to make a determination on any information security topics including establishing a national security policy and standard, then to spread to all ministry departments. The security vision, mission, goal is to be achieved directed by the same standard and policy to every ministry department without exclusion. During the study, the authors also found that not all ministry departments implement the same standard. Therefore, centralisation aspect focuses on all ministry departments to implement the same standard and it is supported by the Ministry of Cyber Defence.

5.1.5 Prioritisation

Prioritisation is to ensure Cyber Security Departments to be a standalone and to be segregated between physical defence and information defence. By having a standalone concept, the Ministry of Cyber Defence is able to focus on the micro aspects with free-lawyers' decisions making process. The Ministry of Cyber Defence is to be separated by other

ministry departments, including the Ministry of Defence or Prime Minister Department or Ministry of Science and Technology or etc., as well as, the Cyber Security Department are to be separated from Information Technology Departments. Information security shall have its own authority.

5.2 Process element

The second P stands for Process which is the process from norm to change. Norm defines as something that is usual, typical, or standard; meanwhile, change defines as an act or process through something becomes different. In the context of this model, process of norm to change is to always answer what norms that can be changed for continual improvement?

5.2.1 Training and awareness level system

The paper contributes a training and awareness level system to establish a learning structure more systematic to enable the participation of every story, and knowledge and awareness throughout the regime. It is to ensure that the knowledge and awareness are reached to every individual. It makes it a learning structure more systematic.

The study found that the current training system mixes every level in a same training session which can be a caused to absenteeism of certain top management. This is the norm side of the culture-minded based on hierarchical system and egoism. The egoism is when leaders are often seen not to jeopardise their own reputation in order to keep themselves higher than the rest, in terms of knowledge and skills. The mind-set of "knowledge and skills make them to be where they are standing now". Therefore, by mixing-up the learning course with the rest of the employees is a treat of jeopardising and gives them a limited-interaction during the course. This is to ensure in keeping themselves balance with knowledge, skill and attitude in front of others. Hierarchy has really effected a socialising and as well as communication. Figure 5 shows a solution. So, the training and awareness level system suggests a learning system by hierarchical, in order to deliver an effective learning plan for information protection in terms of leadership. By changing the norm, it is not only about egoism, but also gaining a reputation as a leader.

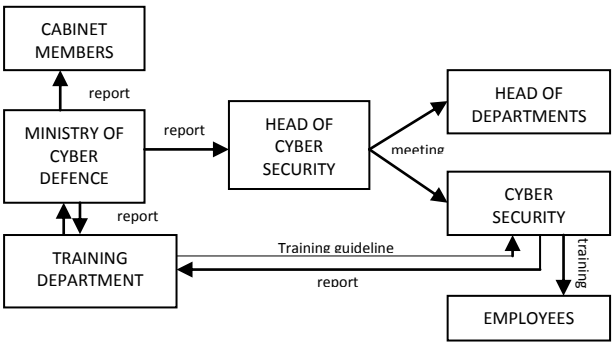

Fig 5 Systematic ways for training and awareness based on hierarchical level

The work also highlights the importance of leaders to understand the employees' security behaviour by analysing their security perceptions. The perceptions help the contents of awareness training which can create an appropriate security amongst employees.

5.2.2 Reflection theory

Leaders are like parents. Children are like mirrors to their parents; hence, employees' practices are a reflection of leadership (Dyana Zainudin, 2015). One quote from unanimous once said "leadership is not a position or a title, it is action and example". In order to continue improving in information security practices, despite knowledge, leaders are also to show commitment in implementing information security. This can motivate employees to follow the example given by their leaders in order to change their daily habit to positive security behaviour. See Fig 6.

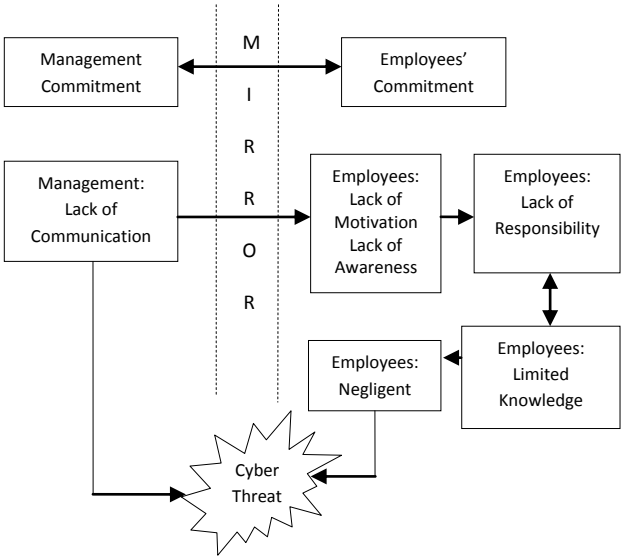

Fig 6 A Concept of Leadership as the Key Aspect of Cyber Threats Prevention (Dyana Zainudin, 2015)

5.3 Product element

The paper contributes three approaches of 3Ts; Tradition, Technology and Technique. These 3Ts are connected to the whole ISO27001 standard processes according to Deming Wheel; Plan, Do, Check and Act. Traditional defines as non-automated tools involved in information security management system; meanwhile, technology defines as automated tools such as software and application medium to ease the process of information security management system. The technique is defined as a way of carrying out an information security management system by following a scientific procedure which has existed in the existing literatures. The combination of existing scientific procedure into technique will benefit the effectiveness of information security management system.

5.3.1 Plan phase

The plan is the process of information security management system readiness involves context of organisation, leadership and planning. In the standard of ISO27001, context of the organisation is to understand the organisation externally and internally. It is as well to understand the needs of the standard and their expectations with interested parties and to determine the scope of the information security management system and its applicability to the organisation.

Leadership in the standard concerns on their commitment towards an information security management system, establish policy, ensure the organisational roles, responsibilities and authorities.

Meanwhile, planning involves actions to address risks and opportunities and information security objectives, and planning to achieve them. All these three parts are involved in a readiness process of information security management system implementation. Table 4 shows a propose solution by the authors.

Table 4 Combinations of three approaches in the product elements of DeGoSec model for plan phase

Traditional	Technology	Technique
ISO27001 Manual Toolkit	ISO27001 Readiness Tools	Doug 7Cs Knowledge Management Capability Maturity Model

5.3.2 Do phase

Do phase involve support and operations. Support consists of five tasks which are resources, competence, awareness, communication and documented information, meanwhile, operations involves planning and controls, risk assessment and risk treatment.

For support, it describes as to determine and provide resources needed for information security management system and it shall determine a competent person(s) throughout the whole process as well as to ensure the awareness in conforming to the standard. Support phase is also to establish communication internally and externally relevant to information security management system and at the same time to document; create, update and control the information related to information security management system.

On the other hand, plan and controls in the operation phase function as to keep track and control the requirements of the standard and to ensure that all changes are to be noted down as a record for consequences review. The rest of tasks in operation phase are risk assessment and risk treatment which to be documented. Solutions that proposed by the authors can be found in Table 5 below.

Table 5 Combinations of the three approaches in the product elements of DeGoSec model for do phase

Traditional	Technology	Technique
Job Orientation Job Description Agreement Training and Awareness Hardcopy Information Security Policies and Procedures	Resource Management Tools Knowledge Management Tools Document Management System Tools	Methods and Techniques Specific to Human Resource Management (Nicolescu, 2009)

5.3.3 Check phase

Check phase involves three tasks which are monitored, measurement, analysis and evaluation, internal audit and management review. Monitoring, measurement, analysis and evaluation are to evaluate the information security performance and the effectiveness of the information security management system such as validate previous decisions; management review decision follows ups are examples for this case, since it is a must to provide evidence that actions you implemented were effective.

It is also to set direction for activities in order to meet set targets; planning, backup activities are a good example, since these data can be used to choose between multiple alternatives. This important as to present factual evidence to justify a required course of action; business cases for updating a firewall or implementing cryptography requires strong and consistent data to sell an idea to management and interested parties as well as to identify a point of intervention and subsequent changes and corrective actions; cause analysis in an access control process problem is a good example of the use of monitoring and measurement data for this reason. Table 6 shows solutions proposed by the authors.

Table 6 Combinations of three approaches in the product elements of DeGoSec model for check phase

Traditional	Technology	Technique
Risk Assessment Meeting Risk Management Training Risk Management using non-automated tools such as Microsoft Excel as a back-up	Risk Management Tools	A Continuous Risk Management Process (Shenkir & Walker, 2007)

5.3.4 Act phase

Act phase includes non-conformity, correction action and continual improvement. This phase functions as to react to the non-conformity and eliminate the cause of non-conformity and to implement corrective action. The information security management system also shall be continually improving the suitability, adequacy and effectiveness of the information security management system. See Table 7 for a proposed solution suggested by the authors.

Table 7 Combinations of three approaches in the product elements of DeGoSec model for act phase

Traditional	Technology	Technique
Governance, Risk and Compliance	Monitoring Security and Performance Tools Incident Handling Tools	Information Security Performance Management Technique Ishikawa/ Fishbone Diagram

6. CONCLUSION

In this section, the authors present a summary of the key contribution of the research. The study discusses the nature of leadership-by-example in information security culture. Leading by example is about influence employees' behaviour. The way how the leaders present themselves affects the success of information security implementation for the whole government. The study has shown that the leaders are to be fully involved in the development and them also to create an effective strategy in managing information security.

A model of key-factors includes Doug 7C's knowledge management as a characteristic that the security leadership should have. The leaders are able to establish a standard of excellence. Leadership-by-example is not about rhetoric, but to deliver. The study suggests the leaders to practice reflection theory which includes in a model of key-factors. The leaders

are able to implement and champion the information security management system.

Leading by example in information security management is to develop a premium communication and decision-making skills. The study suggests a leadership-by-example should have a strategic structure and to be standalone, so to have an actual right to make a decision. Leadership-by-example knows the value of people by captivating the importance of the relationship between the employees will enhance the capability by both leaders and employees in a meaningful way.

Leading by example is not a one-man show. Leading by example creates a strategic cooperation for all parties in managing information security. No matter how brilliant leaders are as individuals, working together with others can create success. Therefore, the strategy of delegating the leadership roles and responsibility should be well planned. Besides security knowledge and security behaviour, leading by example is also about solving issues quickly and effectively. Core security leadership competency is able to understand risk management and involve with the assessment.

Leadership-by-example in information security management system has all about demonstrated the commitment. The leader's commitment reflects employees' commitment. The study summarises the contribution of this paper; the adaptation of leadership in information security culture; developing a conceptual basis for investigating leadership information security; conceptualise the theory of potential non-compliance, security behaviour based on the leadership; emphasising leadership-by-example in developing an information security culture and aligning control according to technology development.

7. REFERENCES

[1] Alhabshi, 2008. eGovernment in Malaysia. *eGovernment in Malaysia*, Volume 18, pp. 1-16.

[2] Cerny, P., 2010. *Rethinking World Politics: A Theory of Transnational Neopluralism.* 1st ed. Oxford: Oxford Scholarship Online.

[3] Dyana Zainudin, A. U.-R. a. B. H., 2014. An Analysis of Top Management Change on Information Security Management System. *Asian Journal of Computer and Information Systems* , 2(6), pp. 177-181.

[4] Dyana Zainudin, A. U.-R., 2015. The Impact of the Leadership Role on Human Failures in the Face of Cyber Threats. *Journal of Information System Security*, 11(2), p. 89–109.

[5] Gams, A. P. a. M., 2000. *E-commerce Intelligent Agents.* [Online] Available at: http://dis.ijs.si/Sandi/docs/ECIAgents.pdf[Accessed 26 April 2016].

[6] Hamid, Thaier KA. "Attack graph approach to dynamic network vulnerability analysis and countermeasures." (2014).

[7] IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management* (2nd Editio.). United States of America: IT Governance Institute.

[8] Karokola, G. R., 2012. *A Framework for Securing e-Government*, Sweden: Department of Computer and Systems Sciences.

[9] Martinez-Moyano, J. R. G.-G. a. I. J., 2007. Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. *Government Information Quarterly*, 24(2), pp. 266-290.

[10] Nicolescu, O. (2009). Methods and Techniques Specific to Human Resource Management. *Review of International Comparative Management*, *10*(1), 5–18.

[11] Ramli, 2012. Malaysian eGovernment: Issues and Challenges in Public. *Department of Politics, Philosophy & Religion, Lancaster University, UK*, Volume 48.5, pp. 1-5.

[12] Schein, E. H., 1992. *Organisational Culture and Leadership.* 3rd ed. San Francisco: Jossey-Bass.

[13] Shenkir, W. G., & Walker, P. L. (2007). Enterprise Risk Management: Tools and techniques for effective implementation. *Institute of Management Accountants*, 1–31.

[14] Stephen Smith, D. B. a. V. P., 2006. *Does Agency Size Affect IS Security Compliance.* Wales, UK, The Tenth Pacific Asia Conference on Information Systems (PACIS 2006).

[15] Von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security*, *25*(3), 165–168. doi:10.1016/j.cose.2006.03.004

[16] Zakaria, O., 2007. *Investigating information security culture challenges in a public sector ogranisation: a Malaysian case*, London: University of London.

[17] Zulhuda, 2011. The State of eGovernment Security in Malaysia.