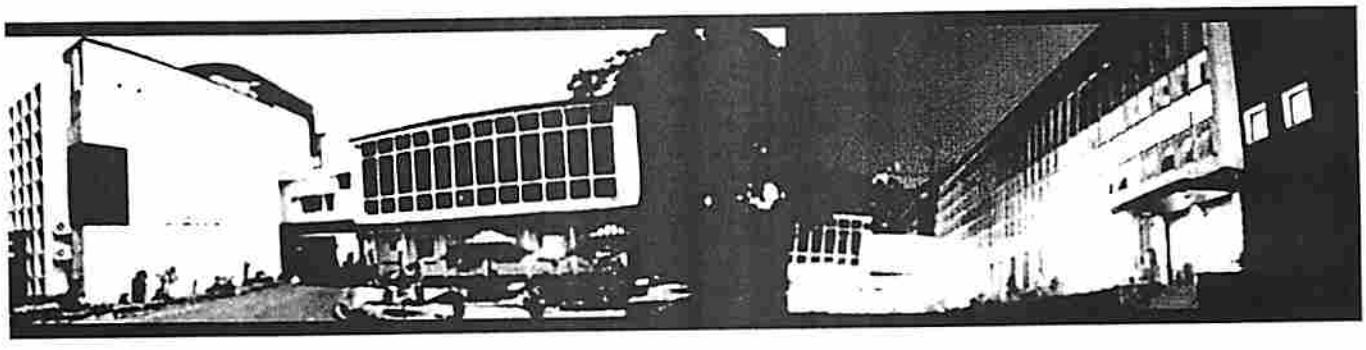

East Hall Auditorium - ITB
Bandung - Indonesia, July 4-6, 2012

Hosted by
School of Business and Management (SBM), Institut Teknologi Bandung (ITB), Indonesia
College of Business (CoB), Universiti Utara Malaysia (UUM), Malaysia

Sponsored by
PT Bank Mandiri (Persero), Tbk., PT Krakatau Wajatama,
PT PLN (Persero), PT Telekomunikasi Indonesia, Tbk.,
PT Angkasa Pura II (Persero), Bank BNI Cabang PTB Bandung

Supported by
Asian Journal of Technology Management (AJTM)
Journal of Technology and Operations Management (JTOM)
Jurnal Manajemen Teknologi (ManTek)

onference Chair
Mursyid Hasan Basri

Editors
Dermawan Wibisono, Akbar Adhiutama, Corinthias Pamatang Morgana Sianipar

TB UUM mandiri listrik pln BARS & SECTIONS Telkom

Committees

The 3rd INTERNATIONAL CONFERENCE on
TECHNOLOGY and OPERATIONS MANAGEMENT (ICTOM 2012)
"Sustaining Competitiveness through Green Technology Management"
East Hall - ITB, Bandung - Indonesia, Wednesday, July 4-6, 2012

TRUSTEE : Rector of Institut Teknologi Bandung

ADVISORY COMMITTEE

Prof. Dr. Sudarso Kaderi Wiryono	Institut Teknologi Bandung (ITB)	Indonesia
Prof. Ir. Dr. Che Sobry bin Abdullah	Universiti Utara Malaysia (UUM)	Malaysia
Prof. Madya Dr. Zulkifli Mohamed Udin	Universiti Utara Malaysia (UUM)	Malaysia

CONFERENCE CHAIR

Dr. Mursyid Hasan Basri	Institut Teknologi Bandung (ITB)	Indonesia

SCIENTIFIC COMMITTEE

Chairman : Dr. Dermawan Wibisono	Institut Teknologi Bandung (ITB)	Indonesia
Members :		
▪ Prof. Dr. Ir. Jann H. Tjakraatmadja, MSIE.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Prof. Togar M. Simatupang, M.Tech., Ph.D.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Prof. Ir. Dr. Che Sobry bin Abdullah	Universiti Utara Malaysia (UUM)	Malaysia
▪ Prof. Kazuhiro Fukuyo, Ph.D.	Yamaguchi University	Japan
▪ Assoc. Prof. Dr. Hartini Ahmad	Universiti Utara Malaysia (UUM)	Malaysia
▪ Assoc. Prof. Dr. Shahimi Mohtar	Universiti Utara Malaysia (UUM)	Malaysia
▪ Ir. Gatot Yudoko, MASC., Ph.D.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Ade Febransyah, Ph.D.	Prasetiya Mulya Business School	Indonesia
▪ Deddy P. Koesrindartoto, Ph.D.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Catharina Badra Nawangpalupi, Ph.D.	Parahyangan University (Unpar)	Indonesia
▪ Yudi Azis, Ph.D.	Padjadjaran University (Unpad)	Indonesia
▪ Wawan Dhewanto, Ph.D.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Eng. Utomo Sarjono Putro	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Ir. Mustika Sufiati Purwanegara, M.Sc.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Ir. Budhi Arta Surya, M.Sc.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Akbar Adhiutama	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Kamal Ab. Hamid	Universiti Utara Malaysia (UUM)	Malaysia
▪ Dr. Rika Ampuh Hadiguna	Andalas University	Indonesia
▪ Dr. Mursyid Hasan Basri	Institut Teknologi Bandung (ITB)	Indonesia
▪ Dr. Norani Nordin	Universiti Utara Malaysia (UUM)	Malaysia
▪ Dr. Norlena Hasnan	Universiti Utara Malaysia (UUM)	Malaysia
▪ Dr. Tony Perdana, SP., MM.	Padjadjaran University (Unpad)	Indonesia
▪ Dr. Mohd. Rizal Razali	Universiti Utara Malaysia (UUM)	Malaysia
▪ En. Faisal Zulhumadi	Universiti Utara Malaysia (UUM)	Malaysia
▪ Ir. John Welly, M.Sc.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Ir. Subiakto Soekarno, MBA.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Ir. Bambang P. Kusumo Bintoro, MBA.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Anggoro Budi Nugroho, S.E., MBA.	Institut Teknologi Bandung (ITB)	Indonesia
▪ Achmad Ghazali, S.T., MBA.	Institut Teknologi Bandung (ITB)	Indonesia

Table of Contents

Available at www.ictom.info

ICTOM

Conference Proceedings © 2012 – ISBN: 978-979-15458-4-6

www.sbm.itb.ac.id

www.cob.uum.edu.my

The 3rd International Conference on Technology and Operations Management
"Sustaining Competitiveness through Green Technology Management"
Bandung – Indonesia, July 4-6, 2012

A Concept of Information Security Management for Higher Education

Puspita Kencana Sari[1,*]

[1]Telkom Institute of Management (IM Telkom),
Jl. Gegerkalong Hilir no.47, Bandung 40152, Indonesia

Abstract. In this information industry era, information is one of important asset for an organization. To run the business, organizations require information that accurate and can be accessed anytime needed. Some of information are confidential that must be protected because it's valuable. Many cybercrimes have happened to steal informations from an organization to make some money or only to make some problem for that organization. Because of that, information security is important for every organization, including higher education institutions. It is not only about protecting information confidentiality from unauthorized access, but also dealing with information integrity and availability. Nowadays, higher education can have a lot of valuable informations, for its internal business process and also external entities. To play its role, called "Tri Dharma Perguruan Tinggi", a higher education can be involved in some researches with industries or government that could be confidential. Besides that, some higher education institution can do some collaboration with others in exchange student program or some research. This cooperation needs some information that should have integration and available to be accessed anytime it's needed. This paper discuss about several types of information to be protected, threats and vulnerabilities of higher education information, and concept of information security management model. This model is adopted form a framework of Business Model for Information Security from ISACA. According to this model, there are four elements that to be considered in information security management; organization, people, process and technology. This is a descriptive research with literature study approach. This paper is a preliminary for the further research of a model of information security management for higher education in Indonesia.

Keywords: Information security, higher education, conceptual model

1. Introduction

Information is one of the most important enterprise assets. For any organizations, information is valuable and should be appropriately protected [4], including in higher education institution. Many information are collected and saved by the universities, such as student information, research, grade, staff and faculty information, curriculum, alumni information, financial information, etc. In this Internet era, organization are

* Corresponding author.
E-mail address: puspita.kencana@gmail.com

most likely to process information by electronic system and give information to their prospect customer by website. This requirement makes universities should have reliable information system.

Security is to combine systems, operations and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organization [4]. By this technological advance, potential threats to the information security are higher. There are many cases reported about information security breach in some universities in USA. Although such a case is almost never heard in Indonesia, most of security breach is occured to commercial or government institution, but it is not rule out the possibility to occur. That is one of the reason to discuss about information security in higher education in this paper. Here, I will use literature review approach to formulate the conceptual model and costumize it to the fact of circumstances in Indonesia.

2. Literature Review

2.1. Information Security Management

The aim of information security is to ensure business continuity and to minimize business damage by preventing and minimizing the impact of security incidents [7]. Information security management is concerned with ensuring business continuity and minimising business damage by preventing and minimising the impact of security incidents that threaten an organisation's information assets (British Standards Institution, 1995). The three basic components of information security are to maintain [8]:

1) **confidentiality** of sensitive information, protecting it from unauthorised disclosure or intelligible interception;
2) **integrity**, safeguarding the accuracy and completeness of information; and
3) **availability**, ensuring that information and vital services are available to authorised users when required.

A threat to information systems can be defined as "circumstances that have the potential to cause loss or harm" (Pfleeger, 1997, p. 3) [8]. This loss could consist of the absence of data or a resource within an information system, financial loss, or loss of company credibility. Threats can either be singular or form part of a combination of multiple threats. Hendry (1995) and Warman (1993) classified information security threats as follows [8]:

- Passive threats are unpredictable natural or physical disasters occurring completely at random, such as fires or floods. It also includes accidental human errors and omissions.
- Active threats are deliberate and malicious attacks on information systems. These can potentially be predicted and avoided. Active threats can be fraud and theft by insiders, malicious code (such as virus, worm, trojan, and logic bomb), malicious hackers, denial of service attacks (DoS) and Social Engineering [9].

Besides to protect their information, implementation of information security by organization is driven by the requirement, such as standardization. The ISO27001 standard provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)" (ISO, 2005a) [3]. The ISO27001 the certification process is driven by either government regulation or the necessity of outsourcing and offshoring in markets. Saint-Germain (2005) argues that an important driver for ISMS certification is demonstrating to partners that the company has identified and measured their security risks and implemented a security policy and controls that will mitigate these risks [3].

Ten key management controls were highlighted in the standard, which constitute the minimum requirements for any organisation. These were [3]:

1) Information security policy document, indicating the goals of information security.
2) Allocation of information security responsibilities by defining security organization.
3) Information security education and training programmes for all staff.
4) Reporting of security incidents, formally ensuring that all employees are aware of procedures.
5) Virus controls implemented to detect and prevent viruses.
6) Business continuity planning, identifying risks to business operations and developing plans to ensure critical business processes continue to run in the event of disaster.
7) Control of proprietary software copying to ensure that only software developed by or licensed to the company is used.
8) Safeguarding of organisational records to protect them from loss, destruction and falsification.
9) Access control to ensure that information is used only for genuine business purposes.
10) Compliance with security policy to be regularly monitored throughout an organisation, and all elements of information security management analysed periodically.

The findings of the present research project suggest that the majority of companies were reactive in managing information security, despite the fact that electronic information was important to the operation of their business. In the event of a security breach, companies were likely, therefore, to be unprepared, and for business damage to be greater than it might have been. It would appear that information security was viewed as a technology problem to be dealt with by technology people. The primary reason that companies were not taking more action to protect corporate information was that they had not yet experienced any major security breaches, especially from the Internet [3].

2.2. Information Security in Higher Education

Higher education institutions are now operating like businesses, managing intricate information security systems. The malware-infected faculty computer at Southern Illinois University exposing 900 student social security numbers and the three stolen laptops at Columbia University led to a data breach exposing over 1400 social security numbers of faculty and staff that could have been prevented [2]. The University of Minnesota was recently attacked, suffering information losses as computers shut down and setting up a chain reaction throughout the state [8].

In May 2005, hackers broke into Stanford University's Career Development Center, gaining access to Social Security numbers, resumes, financial data, credit card information, and government information for 10,000 students and recruiters. In the same month, 380,000 students, alumni, faculty, amployees, and applicants of San Diego State University were affected when hackers broke into four of the university's business and financial services department servers, gaining acccess to Social Security and driver's license numbers. In January 2005, hackers broke into George Mason Uniersity's campus identity card server and gained access to the names, photos, Social Security numbers, and campus ID numbers of 59,000 current, former, and propective students, as well as current and former faculty and staff [1].

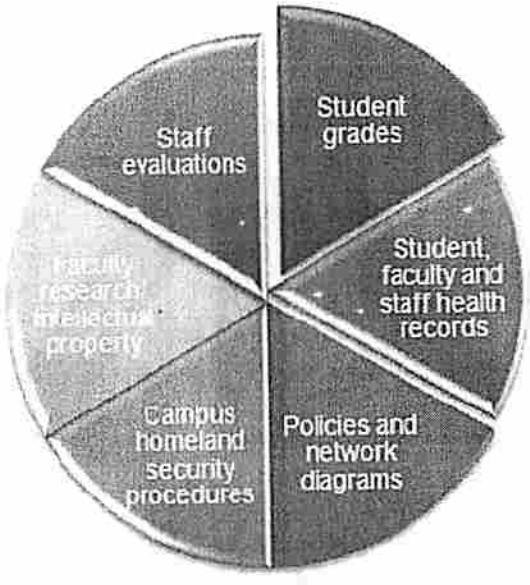

Fig 1: Sensitive Information at Risk in Higher Education Settings [2]

According to Andrerson (2006), some potentially sensitive infromation in universities including: Social Security numbers, grades, financial aid, research, donor information, health records, physical activity, student information, employee information, applicant information, credit card information, communications, e-mail content, and network logins [1]. Figure 1 described some of the sensitive information in higher education institutes are: student grades, student faculty and staff health records, policies and network diagrams, campus homeland security procedures, faculty research, and staff evaluation [2].

Sensitive information is at risk from multiple angles on any given campus including [2]:

- Websites
- Student information systems (front-end web applications, backend databases and the servers they run on)
- Wireless networks—especially open or weakly configured systems

- Network infrastructure devices and even the traffic itself—especially given the prevalence of malware outbreaks
- Laptops and other mobile devices used by students, faculty and staff such as smartphones, iPads, netbooks and USB thumb drives

There are numerous challenges in maintaining security in these areas. First and foremost information security challenge in higher education is limited budgets. Some of the biggest mistakes regarding information security in higher education include [2]:

- Outdated or missing malware protection
- Unenforced email encryption
- Lack of drive encryption
- No preventative controls for data loss

Colleges have become a target of cyber-intrusion for several reason. According to an article in U/S News & World Report, half of universities use Social Security numbers as student IDs, student download music and video that can be an entry point of malicious code or hacker, university databases house lots of personal information and have lax computer and network security, and etc [1].

2.3. ISACA Business Model for Information Security

The Business Model for Information Security (BMIS) presents a holistic, dynamic solution for designing, implementing and managing information security. As an alternative to applying controls to apparent security symptoms in a cause-and-effect pattern, BMIS examines the entire enterprise system, allowing management to address the true source(s) of problems while maximising elements of the system that can most benefit the enterprise[5]. BMIS is primarily a three-dimensional model. It consists of four elements and six dynamic interconnections (DIs). As a rule, all parts of BMIS interact with each other. Elements are linked to each other via the DIs[5].

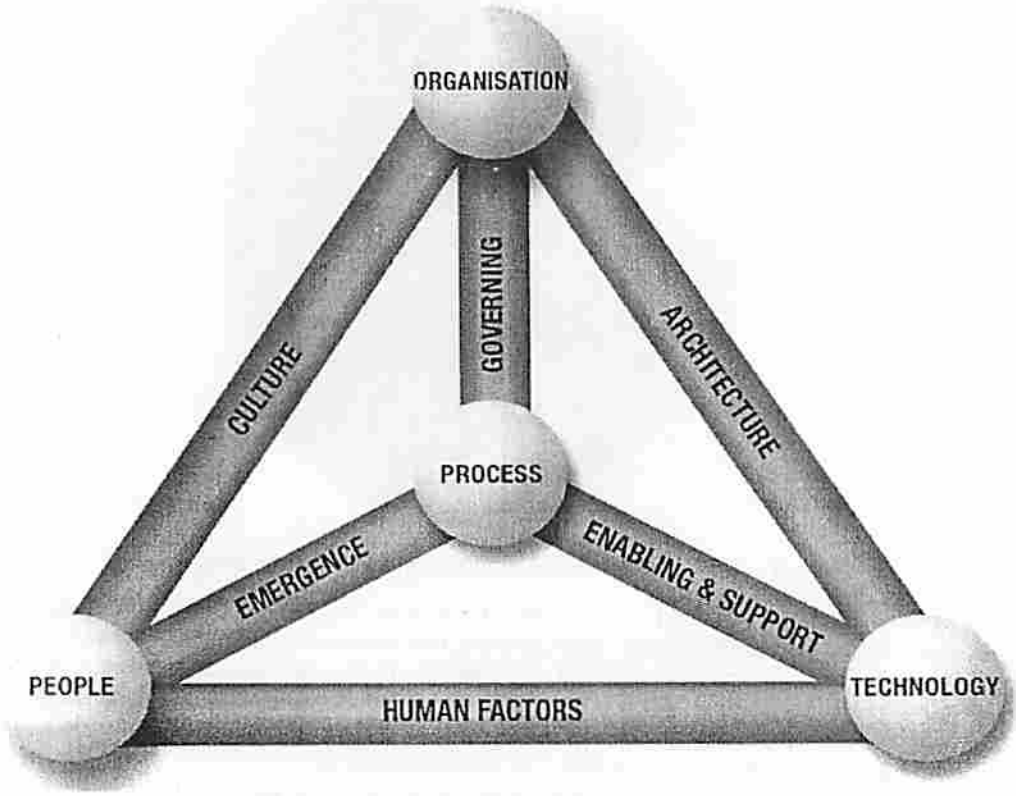

Fig. 2: ISACA Business Model for Infromation Security[5]

The model addresses the three traditional elements considered in IT (People, Process and Technology) and adds a critical fourth element (Organisation). The DIs are Culture, Governing, Architecture, Emergence, Enabling and Support, and Human Factors. In this paper, we only discuss about these four elements.

2.3.1. Organization

BMIS accepts the definition of Organisation as a network of people interacting, using processes to channel this interaction. Within the model's primary circle of Organisation, there are employees and other permanent associates. BMIS also links to external partners, third-party vendors, consultants, customers and other stakeholders. All of these internal and external relationships set the stage for operational effectiveness and, ultimately, the success and sustainability of the enterprise. As part of the BMIS Organisation element, the security programme should be seen as a value center because it enables the business to meet its objectives. Compliance, financial liability and legal issues are all important factors influencing the enterprise. However, they need to be seen in the context of organisational strategy and goals to make sense.

The formal organisation is an important element to any enterprise. In terms of information security it is generally accepted that information security cannot be successful without the support and input of senior management. In many organisations, hierarchical management styles are dominant, so if management does not prioritise security and communicate that priority to the enterprise's people it will prove very difficult to get buy-in from business unit managers, gain adequate funding for the security programme and enforce policy [5].

2.3.2. Process

Processes are created to help organisations achieve their strategy. They are the structured activities that are created to achieve a particular outcome through individual or a series of consistently applied tasks. The Process element explains practices and procedures as people and organisations want them accomplished. Process is a fundamental element that symbolises the requirements for an enterprise to develop, promulgate, educate and enforce security practices and procedures in an ongoing fashion. There may not be a single information security process, and the BMIS Process element will usually consist of a large number of individual processes supporting aspects of security. From the security process perspective, feedback becomes a part of each security process in the model, allowing the specific process to 'learn', improve and adjust over time to respond to changing business environments. Feedback is necessary to adjust to the changing security threat landscape and to support improved security [5].

2.3.3. Technology

Technology can be defined as 'the practical application of knowledge, especially in a particular area' and 'a capability given by the practical application of knowledge'. In the context of BMIS within an organisation, technology covers more than traditional IT. Thus, within BMIS, the Technology element refers to every implementation of technical skill and knowledge that could possibly have an impact on the general security of information. Many information security concerns can be satisfied by the implementation of technology-based controls, including those concerns related to human error or deliberate attack and the impact of natural or man-made disruptive incidents. While there are many options for the tools, enterprise risk and business process risk are the driving forces behind the security programme. Technology selection should therefore always address the utility, efficiency and productivity of the overall enterprise. Once the technology is selected and implemented, training must to be given to those who need to use the tools and monitoring will be needed to verify that the technology is functioning appropriately [5].

2.3.4. People

BMIS's People element represents the human resources in an organisation—the employees, contractors, vendors and service providers. The primary people within BMIS are those who are employed or otherwise associated with the organisation. People within an organisation have their own beliefs, values and behaviours arising from their personalities and experiences. The corporate framework affects, and is affected by, these attributes since it defines its own beliefs, values and behaviours and the degree to which people are expected to comply. In BMIS, the central component that decides on acceptance of controls is People. If employees avoid the process or do not follow the policies, there may be additional risks, as well: When security is seen as cumbersome or too complex, people tend to make their own unwritten rules because they are unable or unwilling to accept the written rules [5].

3. Methodology

To formulate the concept, this paper is used qualitatif method with descriptive approach. Meanwhile, object of this research is information security management (activity) of higher education institution (actor) in Indonesia (place). In collecting the data, it's used some documents from Internet about information security in higher education, including breach cases, requirements and its management. Besides that, it also used observation technique to higher education institution where researcher is located. After collecting the data through literature,

documents and observation, I used domain analysis to get the general and comprehensive picture about the research object. Then, the result from the analysis will be grouped based on elements in business model for information security (BMIS) from ISACA.

4. Discussion

In some higher education institution in Indonesia, information security awareness is still lower than other organization such as banks or commercial institution. Maybe, it's because universities doesn't forced by standard requirement to gain competitve advantage. Implicitly, Indonesia's government has give legal requirement for every organization who has electronic system through Undang-undang No.11 Tahun 2008 about Electronic transaction and information. In Clause 16.b (Penyelenggaraan Sistem Elektronik), it mentions that "every electronic system holder have to protect availability, integrity, otenticity, confidentiality, and accesibility of electronic information in operating that electronic system"[6]. It means that, government force the organization, including universities, to guarantee the information security of their system. But, in fact, this obligation is less of compliance by organization who assume that information security is not too important rather than other IT investment.

According to data (2012) from Directorate of Higher Education, Ministry of Education, there are 3175 higher education institution in Indonesia, state and private. Government, in this case is Directorate of Higher Education, doesn't have legal requirement for the higher education to implement information security. Althoguh some of them, usually top universities, have established a policy about information technology implementation, including point of computer security. But, it still too general and doesn't mention specifically about asset classification, access to confidential information, security officer, or roles and responsibilities for each stakeholder (as in information security policy standard). And generally, this policy is only saved as formal document of organization and lack of socialization to the public user.

Different with the cases of information security in USA, universities in Indonesia do not record students' identity number (such as Social Security number) that become the most reason of security breach in confidentiality. In my observation, most of security breach in that institutions are about information integrity and availability. Most of universities have a website to give information about their institution to the prospect students. But, many of them do not maintain the integrity (completness) and availabilty of related informations. Sometime the website are down or some pages are unavailable. Another vulnerabilities of the information system that can be potential threat are:

- *Natural or physical disaster* like fire or flood. Most of the universities, with limited budget, will allocate their fund to the learning process or another academic process rather than investing on a "good" data center or recovery devices. Some of the them only put their data or network server in a room, with less physical security such as fire detection, etc.
- *Malicious code and malicious hacker.* Like what Beaver (2012) said that security risk in campus came from weakly configured network system and mobile devices from students, faculty, and staff. Some universities have wireless network facilities that can be used by students, faculty and staff anytime in their environment. But, if this technology doesn't equipped by access protection, like firewall or encryption system, it will be susceptible as a hole for malicious code and hacker to get into the university network system.
- *Human error and ommisions.* Some universities have used electronic system in processing their information, including academic system, library system, etc. If the user doesn't familiar with those system, or there is less access control into that system, it can breach information integrity.
- *Social engineering.* One of the common type of social engineering is phishing where an outsider pretends to be an official site that ask personnal information by email. This could be occur because usually universities give an official email account for every student, staff, faculty, or even alumni.

Although universities in Indonesia do not record such a Social Security number, they still record some information that shoul protect their confidentiality, integrity and availability. According to regulation from Directorate of Higher Education, every higher education institution should report some information for each semester, called EPSBED (Evaluasi Program Studi Berbasis Evaluasi Diri/ program study evaluation based on self evaluation). This report contain some informations such as:

- Students' personal information
- Students' transaction information (leave, graduate, or drop-out)
- Students' grade
- Curriculum
- Faculty information

- Publication information
- Facilities and capacity information

Besides those informations above, universities also have other confidential information that can has restriction access, including:

- Financial information,
- Examination file; some institution apply a procedure where faculty have to send examination paper by email to academic staff ,
- Students' bank account; especially for institution who has cooperation with bank for student registration payment by auto-debet,
- Universities strategy,
- Internal memo for faculty and/or staff,
- Employee information, etc

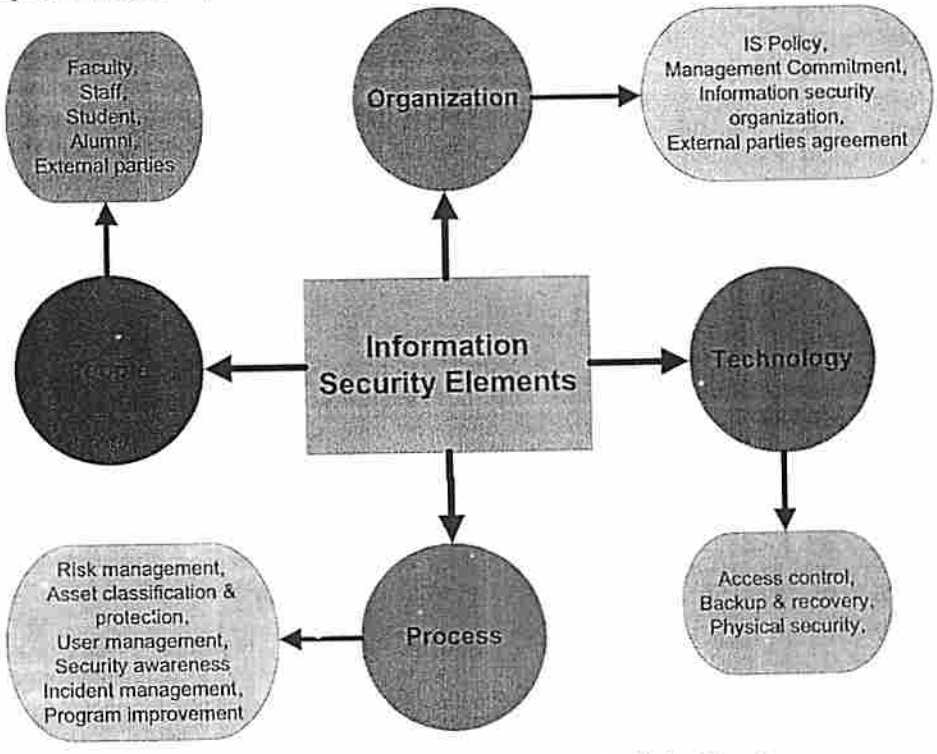

Fig.3: Conceptual Model of Information Security in Higher Education

After discussing type of informations and potential threats, in figure 3 we discuss about conceptual model of information security management, adopted from ISACA Business Model for Information Security. In this paper, we only discuss about four information secutity elements, excluding the dynamic intersections. From those elements, we will break one by one to be some points that to be considered by higher education institution in implementing information security.

1. **Organization**. First point is information security policy that should be established when instituion want to implement their security program. That policy should comply with institution's objectives. Next important point is commitment from senior management to support the implementation of information security program. By that support, management will allocate organization resources needed to succeed this program. Third point is information security organization. It should be a clear roles and responsibilities in the organization structure that commit to information security programs. This roles also give a clarity who should be contacted when there is incident of security. It would be better if the university has at least one person to be a security officer. Or, they can assign available staffs to play the roles. Another point to be considered is agreement with external parties, such as service providers. Institutions should clearly define about their rights and obligation and access to the institution's system. So, if they do some activities that can be risky for the security, they can be given a penalty.
2. **Technology**. To support the implementation of information security, institution should apply tools and knowledge for access control, backup and recovery, and physical security. Access control tehcnology is

needed for managing who can access what information or part of systems. Backup and recovery technology is needed to prevent data loss if there is incident or disaster that interrupt system operation. While physical security is for protecting the system physically.

3. **Process.** In the process element, there are risk management, asset classification and protection, user management, security awareness, incident management, and program improvement. Risk management are held to assess what potential security risk for the institution so they can define what program are suitable to manage that risk. Another process is classify the information asset, which ones are confidential, which ones are for internal, and which ones are for public consumtion. By that classification, institution can apply suitable program protection for each asset group. User management process is needed to manage user access to the system, including authentication and authorization. Security awareness is also an important process to support the security programs bv building behaviour of people. Incident management process is used to handle when there is security breach. And last but not least, it's needed program improvement where organization should hold evaluation periodically and gain feedback from security programs that have been run. By this improvement, organization can adjust its protection with potential threats that always evolve.
4. **People.** This element represent human resources in organization, in this case, people elements in higher education that should be considered are faculty, staff, student, alumni, and external parties. Faculty, student, and staff are common human resources in universities. But, alumni is only for those who still give access for using some resources, such as email, alumni system, or e-learning. While external parties could be vendor or partner who cooperate with universities for particular systems, such as career and development center system.

5. Conclusions

Information security is important for every organization, including higher education institution. It is not only about protecting information confidentiality from unauthorized access, but also dealing with information integrity and availability. Nowadays, higher education can have many valuable information, for its internal business process and also external entities. This paper has discussed about several types of information to be protected, threats and vulnerabilities of higher education information, and concept of information security management model. This model is adopted from ISACA Business Model for Information Security. According to this model, there are four elements that to be considered in information security management; organization, people, process and technology. While six dynamic intersections (DIs) from that model is not considered in this paper.

This paper is a preliminary for the further research of a model of information security management for higher education in Indonesia. For the next research, we can do more observations and interviews to private and state universities to customized the conceptual model and analyze more in type of confidential informations and potential threats. Therefore, key success factors and obstacles to implement this model in Indonesia cannot be concluded now because it needs more research. By this model, hopefully can help higher education instituion in implementation of information security programs.

References

[1] Anderson, A., (2006). "Effective management of Information Security and Privacy. *EDUCAUSE Quarterly*. No. 1

[2] Beaver, Kevin. (2012). "Information Security in Higher Education". Accessed from www.sophos.com in May 25th, 2012

[3] Gilies, A., (2011). "Improving the Quality of Information Security Management Systems with ISO27000". *The TQM Journal* vol23 No.4, 2011 pp 367-376. Emerald Group Publishing Limited

[4] Hong, Kwo-Shing., et al., (2003). "An Integrated System Theory of Information Security Management". *Information Management & Computer Security* 11/5 [2003], 243-248. Accessed from www.emeraldinsight.com/0968-0277.htm. in May 25th, 2012

[5] ISACA. (2010). "Business Model for Information Security". USA. Accessed from www.isaca.org, in May 20th, 2012

[6] Kemenkominfo. (2008). "UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik". Accessed from http://www.pemkomedan.go.id/uuti/uu_112008.php in May 28th, 2012

[7] Kruger, H., *et al.*, (2010). "A vocabulary Test to Assess Information Security Awareness". South African Information Security Multi-conference in Port Elizabeth, South Africa. Accessed from www.emeraldinsight.com/0968-0277.htm. in May 25th, 2012.

[8] Mitchell, R.C., *et al.*, (1999). "Corporate Information Security Management". *New Library World* Vol 100, Number 1150 pp 213-227. MCB University Press. London UK ISSN 0307-4803
[9] Peltier, Thomas R., et al, (2005). "Information Security Fundamentals"., CRC Press LLC
[10] Solms, R.v., (1999). "Information Security Management: Why Standards Are Important". *Information Management & Computer Security* 7/1 50-57. MCB University Press. ISSN 0968-5227.

Cite this paper

Sari, P.K. (2012). "A Concept of Information Security Management for Higher Education," *Proceedings of The 3rd International Conference on Technology and Operations Management: Sustaining Competitiveness through Green Technology Management*, Bandung–Indonesia (July 4-6), pp. 639-647. ISBN: 978-979-15458-4-6.