A Review of Effective Knowledge Management System for Control in Mining Industry in Thailand: A Case in Point

Phanu Waraporn*

Abstract

The availability of effective knowledge management systems is considered to be now very vital when coping with today's dynamism and complication both within and surrounding organizations. However, due to small implementation of Knowledge Management systems in this industry, this becomes disappointing. Either the projects do not produce the results that organizations desire or the added value of the implemented technology seems limited or unreachable. This paper explains the effectiveness of having a knowledge management system in place for the overall economical aspects and control of the firms. As a result of literature review and past experiences, we can identify shortcomings of current methods, techniques, and supporting technologies. Based on preceding concepts, four design guidelines for the specification of effective knowledge management systems are proposed. The application titled Enterprise Information Portal (EIP) is now being undertaken at a disclosed mining company in Thailand as a case study.

Keyword : Knowledge Management, Management Information System, Information Systems, Business Control, Mining

1. Introduction

The increased interest in knowledge management reflects the shift from serial to parallel experimentation in the laboratory and is the key to accelerating product development and commercialization. Primary goals are process improvement through sharing of best practices, and the sharing of what is called "tacit knowledge" or the undocumented expertise of workers – a firm's technical and work skill folklore. Yet at the same time, document management systems and other database software facilitate a sharing of information among the "silos" of a company that does not normally exchange information readily. Much more than that and importantly enough is now knowledge strategies are beginning to address control issue. So the best measure of the effectiveness of knowledge management is the end of the pipeline informing decision makers prior in advance in order for them to be ready at any time to detect and prevent avoidable problems and mitigate the effect of the inevitable.

Information technology has become a way to provide managers with information. The developments of Management Information Systems (MIS), Decision Support Systems (DSS), Executive Information Systems (EIS), Data Warehousing and Mining (DW/DM), Data Visualization (simply data-analysis tools), ERP and CRM systems, Knowledge Management Systems (KMS) and Enterprises Information Portal (EIP) resulted in a collection of systems, all of which are intended to support management with a new or better information.

The above means not only millions of Baht being spent but also the time, efforts and endeavors deployed to have systems up and running. Nevertheless those do not guarantee that information will contribute to an improvement in organizational performance.

Field experiences endorse that practical and effective guidelines and approaches for the delivery of reliable information for management decision using enterprise information portal based on the Knowledge Management System Framework and Architecture are gaining great challenge for an organization to stay afloat and on top of competitors.

This paper begins with analysis of the constraints surrounding information management concepts and its uses. It then synthesizes the field experiences and from available literatures into guidelines. As a matter of fact, the paper aims to contribute to the general understanding of known facts of problem in practically delivering the effective knowledge management and propose ways toward defining and fostering the successful implementation of Enterprise Information Portal of the mining industry.

2. Management Information Constraints

There are four constraints surrounding management information according to Lohman et al. [1], 1) data availability and quality does not meet requirements, 2)requested and provided information are unrelated, 3) poor self-assessment of information needs, and 4)information use does not contribute to organizational performance.

To better prevent management from rendering wrong decisions based on incorrect data being entered, data availability and quality must meet specific requirements. This usually involves data entry personnel, intrinsic value of the data and the way data being stored to derive and support not only for primary processes but also the decision making processes [2].

The information provided and available may be too much to be analyzed and therefore manager cannot distinguish between relevant and irrelevant information [3]. Sometimes due to technological push phenomenal that overwhelm management with new gadgets to improve management information from IS function. In addition, the missing link between provided and requested information might be a lack of proper communication. For example, manager does not have time to give proper instructions or requirements to system analysts.

There are five causes of poor self-assessment of information needs; managers may not be well trained to manage; analytical capabilities and way of working of the manager could play a role; cultural or institutional properties of an organization may produce discrepancies between desired and required information; the intentions behind gathering information are not always to solve problems or to support decision making as it is basically used to justify decisions that have already been made; and lastly people appear to satisfice rather than trying to optimize. In order to cope with this, an

*Department of Information Tecnology, Faculty of Information Tecnology, KMITNB

understanding of psychological aspects of individuals is needed.

In quite a number of cases, information use does not contribute to organizational performance. This is despite the fact that information is power, providing good information may be a harmful thing as it might affect certain individual vested interests. In fact people always think about themselves more than the organization. Todd and Benbasat [4] found that managers are more concerned with time reduction than quality improvement of the decision-making process.

In summary figure 1 in the next page depicts the four constraints graphically in relation to each other. The numbers refer to the constraints presented above.

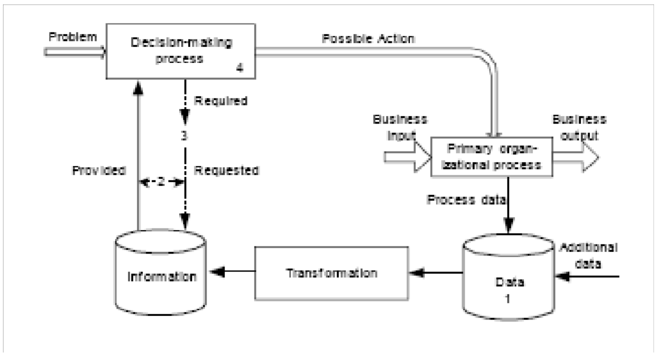


Fig. 1. Positioning of the four constraints.

3. Perspectives on Knowledge Management Information Generation for Mining Industry

Based on Lohman et al. [1], the literature shows that generation of effective knowledge management should not be covered by a single discipline. Management science, organizational science, accounting, operational research, computer science, statistics, engineering and mining contribute to the understanding of this process. Nevertheless, the research areas of each discipline are not strictly separated. Though each one has its own view, they overlap in many aspects. To structure the research area, four different perspectives: the data, statistical, specification, and information system perspective are being defined below.

Data Perspective-The enormous amount of data generated by primary processes is seen as a gold mine that can be capitalized upon. Data is perceived to be truly unparallel assets and for which competitors are incapable of duplicating. Thus the primary objective of the system and related technologies is to make the data accessible for all (of course with reservation that data and information are being classified and available to those permitted) and let it be turned into information and subsequently new knowledge. The process goes iterative and new and further knowledge is created.

Statistical Perspective-As we are all aware, data can also be analyzed to find relationships or patterns (most of the times new knowledge) within the data and that could be further used to the advantage of the decision maker. These analyses are made using statistical methods and techniques. The question is how to cope with the unexpectedness and the actionability. In most cases we are unable to define the actionability so that it can turn the unexpectedness or result of the statistical information into actions.

Specification Perspective-Specification are methods used to determine requirements. The process of requirement analysis is view as most important stage of any system development life cycle. The analyses can be in any form of the three approaches; asking, critical success factors and balance scorecard. The analyst obtains information requirement entirely from persons in the organization by simply asking them what the exact requirements are. However this could be misled as already mentioned in the previous section due to personal interests etc. The CSF tries to determine the key areas that dictate the organizational success. Unfortunately, the CSF method does not try to deal with needs for strategic planning but for control needs to monitor and improve existing process. The balance scorecard is a set of four measures, namely, financial and operational, customer satisfaction, internal process, and innovation and improvement activities. All these methods can be structured but the quality of the real requirements lies heavily on the vision and competence of the persons giving out the analyses and comments. Furthermore, the results of the three methods are a mere straightforward indicator on descriptive statistics or simply a focused strategies instead of full requirement analysis but the real value using more complex techniques to derive other types of requirements is basically ignored.

Information Systems Perspective During the past decades several information systems have been introduced to support management. However it is not clear as to the characteristics, uniform definition, indistinct and more than one framework are used to define the same type of information system. It is still an issue to further analyze the aforesaid to come up with universally accepted and of our own definition. Whatever it is, all the systems are designed to improve the efficiency and effectiveness of management by using information technology. They are all information systems supporting decision process as per Sol [5]. This perspective overlaps with others and is meant to imply that most comments given in previous paragraphs are also applicable on this issue. The only complication is that if the management information only indicates discrepancies between results and formulated goals but does not include directions for actions to eliminate the discrepancies, the information does not contribute to the improvement of the organizational performance.

4. Design Guidelines

Guideline 1: Develop, formulate and elaborate control instruments and their organizational context (control model) as a starting point for deriving information requirements on knowledge management systems

Guideline 2: Develop, formulate and elaborate mission and goals of the organization and use them as reference points for constructing a control model

Guideline 3: Knowledge management requirements must initiate the configuration and the specification of the data to be stored.

Guideline 4: The development of control models, the specification of the information requirements and the configuration of the appropriate technologies to derive the information should be an iterative process with a balance between feasibility and desirability.

5. Case in Point Summary and Future Works

The mining company in this review paper has been in business for nearly a century and has gone through various stages of change in both ownership and the way the business is operated. It has operated three different mineral resources mining sites throughout the country. Being listed in the stock exchange of Thailand, new international compliance requirements and with future expansion plan, in order for it to better manage its economic resources, the central knowledge management systems for control is being firstly viewed as a way to conduct current and future businesses with hassle free and be able to support management and its personnel through new knowledge acquisition, capturing, transferring, sharing and creating. . We analyzed the existing systems, management and meeting reports, and conducted interviews. Using constraints in section 2 as a framework and through time limitation, we identified and classified issues that this company was facing to a certain degree.

In applying guidelines as proposed in section 4, we believe that if more detailed studies are being carried out and guidelines are strictly adhered and followed, the effective knowledge management systems for control using Enterprise Information Portal could be generated and fruitful to the company as a whole. For example, if a business analysis was conducted to get an understanding of the organizational characteristics and processes, the result would be the application of different perspective to derive required information. A technology perspective was used to apply and build (prototype) systems to get the desired information. Lastly using statistical knowledge to validate the outcome from that prototype

6. Conclusion

In this review paper we have elaborated the availability of effective knowledge management systems from a control perspective. There are four problems that prevent the construction and the use of effective knowledge management system. Application of various available technologies and theories does not seem to get the problems solved.

The unsuccessful trial and errors to establish the requirements of effective knowledge management systems lined on clear organizational requirements. This costs not only a lot of resources wasted, but also failure to deliver value for organizational control may cost significant performance improvements too. The lesson learned from both field works and through literature should then be used to prevent other future implementations from the same obstacles and mistakes. In finally conclude, we recommend that the process of rethinking is a must do and a more emphasis be placed on the primary processes which should be led to the Business Process Reengineering can then the current technology be effective as in line with current practices rethought. Vast technologies and new jargons like data mining would mean nothing unless business data is being reestablished through the process called Business Data Reengineering. The recommended four guidelines explicate the most essential change needed to derive effective knowledge management systems.

References

[1] Lohman et al., The Illustration of Effective Management Information: A Critical Perspective, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

[2] Tayi, G.K., D.P. Ballou, Examining data quality, Communications of the ACM, Vol. 41, No. 2, pp. 54-7.

[3] Simpson, C.W., L. Prusak, Troubles with information overload moving from quantity to quality in information provision, International Journal of Information Management, Vol. 15, No. 6, pp. 413-25, 1995.

[4] Todd, P., I. Benbasat, The use of information in decision making: an experimental investigation of the impact of computer-based decision aids, MIS Quarterly, Vol. 16, No. 3, pp. 373-93, 1992.

[5] Alter, S., Information Systems: A management perspective, The Benjamin/Cummings Publishing Company, California, 1996.

Information Assurance Education A Critical Element for Advancement

Mark Weiser*

Abstract

Information assurance (IA) is imperative to business expansion, particularly as ties are made between businesses and consumers, as well as between countries. There is a global shortage of IA workers, which is even worse among Southeast Asian countries. Information security is no longer a luxury, or can it be an afterthought to be added to systems after design and implementation. Educational institutions must begin to add or integrate IA programs within their institutions, to provide their graduates as critical tools that fuel growing businesses and economies.

1. Introduction

Many people do all of their banking online, we and our children communicate with peers through computer systems, and there are many jobs that require near continuous interaction with computer systems. Criminals, however, are also "connected", and our online interaction provides them a conduit into our information like never before. Rarely does a day goes by that we fail to hear of some new computer security breach. Our credit card numbers are at risk, our children's personal information is exposed to the world, and our professional reputations are on the line. We expect network and service providers to protect against these things, without us having any impediments at all. This is a difficult task, but a critical balancing act for those companies that will be successful in the marketplace.

Thailand is no different the technological infrastructure is in place to connect and do business with the rest of the world. High-speed connections both for academia and private industry exist through multiple neighboring countries. Pure engineering is no longer the issue to move rapidly forward. A firm foundation of information assurance knowledge in the workforce and consumers is now necessary to have the credibility to best use those broadband links.

Thailand need not reinvent an approach for educating its students in this critical area. A long history of development and refining information assurance curricula exists in the United States and other countries. These materials are available and can be leveraged by Thai educational institutions to rapidly integrate critical learning objects into existing coursework. We, as academics, must provide the right education to our students for them to understand the issues in information assurance, address them with innovative and cutting edge approaches, and provide solutions that meet the business need and enhance productivity and/or profitability.

This paper looks at why it is particularly important to have an information assurance curriculum in any country, but particularly one like Thailand that is poised to economically move up among its peers. The paper reviews various models of security that might be brought to bear on the development and implementation of an information assurance program, and then illustrates an example curriculum which has the flexibility to be applied to both technical and non-technical programs. It is the author's belief that providing firm security education is no longer an option for institutions of higher education anywhere, and hopes that this paper will assist in establishing programs that prepare the next generation workforce to aide in developing a flourishing economy on a safe platform.

2. Importance of Information Assurance Education

A continuing and increasing challenge facing developed society is the security and protection of our information assets. The ability to connect to vast amounts of data at high speed from businesses and homes is increasing worldwide, however, direct attacks and malware undermines confidence in systems and the data accessed. The ability to do business with others within and between countries is compromised by a lack of trust between systems.

One of the most important and long-standing concerns facing the global economy is "the threat of cyberterrorism and the vulnerability of the nation's information systems and communications networks … The need we all recognize, for a cadre of professionals in computer security and information assurance is at the top of the list" [1]. It must be recognized that only "an educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure" [2].

2.1 Increased Connectivity

The information economy now drives much of the global wealth. Network capability and connection is critical to competing in this marketplace. Everything from credit information to digital products flows over data networks. This makes Internet connectivity a key indicator of potential for economic growth both between companies, as well as to the end consumer.

In the United States, broadband penetration exceeds 65%, among active Internet users. This is actually only the 19th highest rate worldwide, with many Asian countries rapidly adding consumer broadband capacity. Hong Kong leads Pacific Rim countries with over 73%. Even China is poised to pass the United States in terms of total broadband subscribers late this year.

Thailand's broadband penetration is relatively modest at 1.7%. It is important, however, to look at total Internet penetration and growth trends for an economically developing country. Thailand's total Internet penetration is 12.7%. It's only neighbor that is higher is Malaysia at 36.7%. Because of the obvious economic disparity, is no surprise that Thailand far exceeds Myanmar (0.1%), Laos (0.4%) and Cambodia (0.3%) [3]

Growth of overall Thai Internet penetration has increased 266% in the first six years of the decade, with is small compared to other developing countries for the same period. Those

*Center for Telecommunications and Network Security, Oklahoma State University connected to the network, however, are rapidly increasing their bandwidth use. Figure 1 illustrates the traffic growth in Thailand. Total combined domestic and international consumed bandwidth went from 712 Mbps in January, 2000 to almost 48.6 Gbps in April, 2006 – a total growth of 6800% or an average growth of almost 90% per month [3].

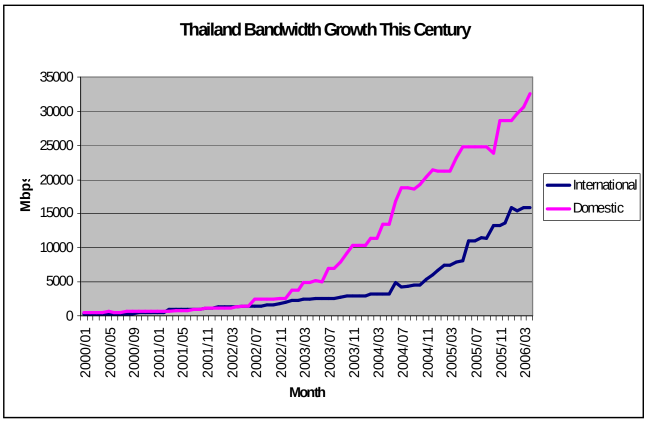


Fig. 1. Internet Traffic Growth in Thailand. From [3].

2.2 Vulnerabilities Increasing

Sustaining such rapid growth is difficult and may lead to shortcuts in security and other controls. Even properly informing the user community is difficult, when large numbers of new users join the network daily. Internet vulnerabilities, however, are increasing in severity and speed.

The 2005 CSI/FBI Computer Crime and Security Survey [4] revealed an average loss by the 639 respondent companies of over $203,000 from IA-related issues. Every one of these companies had a formal internal security function. Without that, the number would be significantly higher. 75% of these companies do not insure against cyber security risks, meaning their only safety net is the qualifications of their security staff.

Viruses and other Malware dwarfed the other areas of loss, comprising almost $67,000 of the average loss. Most viruses and worms, however, affect companies long after a patch is available, and it is simply the negligence of the consumer or company that leaves the vulnerability open to an attacking agent. For instance, the NIMDA worm was released on September 18, 2001 and shut down major portions of the Internet. Microsoft patch MS00-078 entirely addressed the issue that made the exploit possible, and was released on October 17, 2000 almost a year earlier.

Although not consistent, the trend is for attacks to occur soon after a vulnerability is recognized, announced, and patched. Figure 2 depicts the decline in time from patch to exploit. In November, 2004, Microsoft and its users were taken by surprise when the MyDoom.AG hit. From the time of the exploit, it was 23 days until a patch was available. The potential for attacks prior to vendor awareness or patching is very real, and must be addressed by a skilled group of information assurance experts in user companies to avoid long-term outages and extreme financial loss.

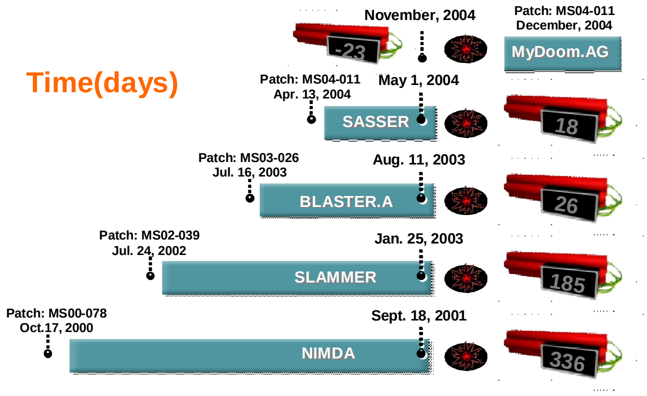


Fig. 2. Days Between Patch and Exploit. From [5].

2.3 Security Employment

Ultimately, higher education is geared to equipping students to enter the workforce. Thailand's 2005 GDP per capita was $8,300, relative to the US's $41,800. [6] Compensation for security jobs is among the highest of any area for college graduates. According the 2005 SANS Information Security Salary Survey [7], the worldwide median income is $77,050 for security professionals. That, however, is skewed by high salaries in a few countries. Removing the US, Great Britain, and Canada, leaves a median IA income for the rest of the world of $51,250, which far exceeds the average GDP of these countries.

Because of the shortage of educated information assurance professionals, even those with less than three years of experience earn an average of $63,529 in the United States. If the ratio holds for other countries, this implies that a novice IA worker outside of the three aforementioned countries would make over $40,000 per year. A relevant masters degree increases that by another 17%.

Most technology fields have the concern of outsourcing of jobs, should local salaries increase too much. Because of the sensitivity of information assurance, these jobs most often remain with the company which is trying to project its information assets. 63% of companies in the FBI survey [4] outsource none of their security function, and only 10% of the companies outsourced more than 20% of their security function. These jobs are considered critical to keep in-house, providing IA workers job security unlike that felt in any other area of information technology.

2.4 Thailand Economic Implications

Security is important wherever you live. This is true with physical security, economic security, and emotional security, among others. Thailand is considered a "Developing Economy". Fortunately, however, the country is near the top of that list in terms of GDP Thais have incomes that far exceed some of their poorer neighboring countries, but Thailand is still far from being classified as a "Developing Economy," such as that in Korea, Singapore, and Taiwan.

The focus has been on growth, economic development, and establishing ties to the commerce in the West. This creates a fast moving technology development cycle which is prone to neglect security. The opposite approach, however, is absolutely necessary for the country to improve in today's digital economy.

Foreign interest in developing countries is primarily as a source of inexpensive manual labor. Movement to a knowledge-based economy, with accompanying higher wages, requires technological linkages with other countries. A prerequisite to this is proper investment in network security to prevent risking the infrastructures and information of those foreign investors. Thailand must educate sufficient numbers to meet the growing demand for an IA workforce to enable the potential for economic advancement within the world economy.

3. Curriculum Models

The argument for increasing education in information assurance is very strong, but it is not as clear how it should be accomplished. Because information security is very much an evolving discipline, there are almost as many different curricula as there are programs. Because most US university programs grew from a government initiative, a strong culture of sharing curriculum developments was fostered. Much of the resulting coursework is publicly available on the web and through published conference proceedings and journals.

3.1 Standards Bodies

Most disciplines in the US have a standards body which sets general curriculum guidelines and standards for programs. That is not the case in information assurance, although there are several ongoing initiatives to incorporate related program standards into existing structures. It is likely that various academic disciplines (Computer Science, Engineering, MIS, etc.) will eventually each have their own "standard" for IA education, although they will likely overlap significantly.

Perhaps the greatest struggle between competing faculties is the question "Where should information assurance exist?" For this, we can look to the ACM's Special Interest Group for Information Technology Education's "Computing Curriculum: Information Technology Volume" [8]. This joint project between IEEE and ACM references CC2004 for four different degree programs in computing: Information Systems; Software Engineering; Computer Engineering; and Information Technology.

In US educational institutions, there are three possible departments that are likely to house an information assurance discipline: Computer Science; Engineering; and Management Information Systems. Classically, computer science focuses on issues of software and programming and engineering deals with the physical construction of the components necessary for an implementation. MIS focuses on taking a business risk or opportunity and designing a system-based solution, which would then be implemented by computer scientists and engineers.

Any of these disciplines may be home to information assurance. It depends on the emphasis that the institution wishes to have. Many of the tools that provide system and network security are software solutions, implying that Computer science is at the core. As the amount of processing and network traffic increases, pure software solutions become inadequate meaning they must be moved to firmware and hardware solutions the purview of engineers. Even the term "Information Assurance" implies protection of a valuable corporate asset. That may require the coordination and cooperation of business management, computer scientists, and engineers, indicating that MIS may be the appropriate location.

One thing that is clear from the Computing Curricula draft is the importance of IA education in any or all of these related disciplines. Information Assurance and Security is the only area that is considered an "IT fundamental," a "pervasive theme," and a complete "knowledge area." IA is clearly considered a real and important discipline, regardless of its academic home.

3.2 Major Curriculum Models

In many areas, professional certifications grow from academic disciplines. This provides a common metric that crosses universities and allows comparison between graduates of different institutions. Widespread implementation of IA in higher education was very slow, and industry demanded the availability of measurable IA training for the workforce.

The International Information Systems Security Certification Consortium (ISC)^2 is internationally recognized for educating and certifying information security professionals. Over 40,000 information security professionals in 100 countries have been certified by this organization. [9] Academic programs have certainly built on the 10 common bodies of knowledge (CBK) on which this exam is based:

1. Security management practices
2. security architecture and models
3. Access control systems & methodology
4. Application development security
5. Operations security
6. Physical security
7. Cryptography
8. Telecommunications, network, & Internet security
9. Business continuity planning
10. Law, investigations, & ethics

Most overview security textbooks cover each of these topic areas to varying degrees. We must not stop there. Valli [10] contends that universities that conform primarily to the certification standards available, risk replacing sound foundations of their discipline with technology-specific data, which will rapidly become obsolete:

"Universities should consider with gravity, what it is that they are trying to achieve... This total curriculum replacement via industry certification substitution path is perilous and will see universities becoming vendors savants."

As a compliment and guide under their curriculum, however, the 10 domains can serve a university's faculty well.

Another guiding factor to the growth of IA programs in the US has been federal government certification standards. These, in fact, become a primary criteria for designation as a National Center of Academic Excellence in Information Assurance Education. As a result, most schools with full IA curricula map their courses to these federal standards.

Rather than being knowledge or skill based, such as the ISC CBK, these standards relate to specific roles that an IA professional may hold. Guided by the National IA Education and Training Program [11]. These areas include:

1. INFOSEC Professional
2. Designated Approving Authority
3. System Administrator in Information Systems Security
4. Information Systems Security Officer
5. Systems Certifiers
6. Risk Manager

Unlike the ISC CBK, these titles do not provide a good indication of the requirements in each area, however, each has over a hundred items of information that is specified to meet the standard.

3.3 A Guiding Security Model

The model for information assurance that is most often cited among the 66 US National Centers of Academic Excellence in Information Assurance is that proposed by Machonachy, et al [12]. Figure 3 provides a visual representation of this model, showing the intersection of information states, with the security service and countermeasure applied to it. This "cube" structure is easy to understand by students, but also may serve as a guide to assist faculty in determining relative emphasis in their degree programs. For instance, a faculty of Business might focus on People, Policies and Practice, where Engineering would look more at technology solutions. None of the areas should be neglected, however, nor should the relationships between them.

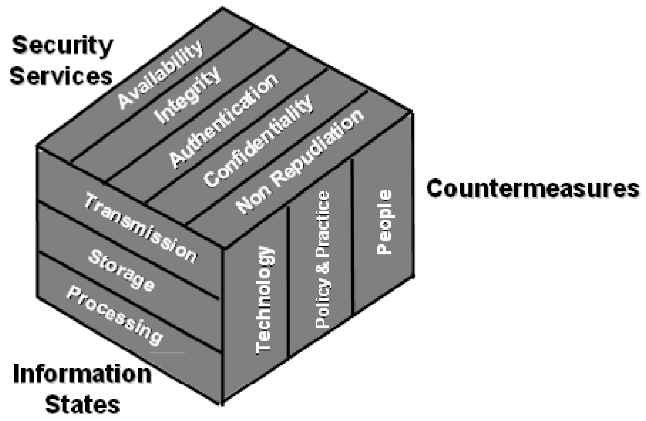
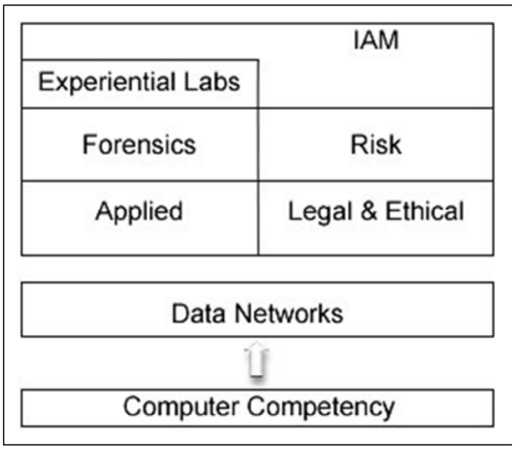


Fig. 3. An Integrated Information Assurance Model. From [12].

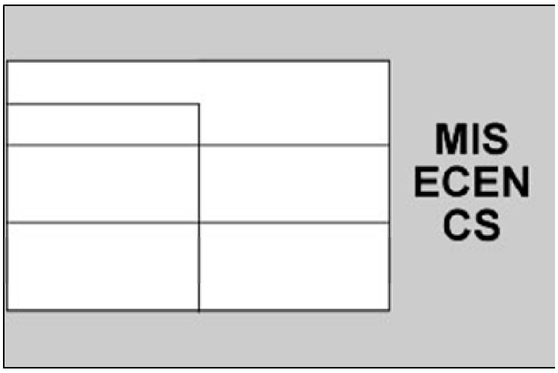
4. An Example Curriculum

The author knows of no two schools in the United States that have implemented an information assurance curriculum in the same way. Most, however, use a combination of the Machonachy model, the ISC CBK, and the NSTISSI/CNSS standards to ensure a complete curriculum. The following curriculum is one used in the author's home institution. The goal for this curriculum is for it to be both accessible and extremely useful to students from almost any major. It can stand alone as a minor or certificate, or can be used within several major programs as a formal option. Additional details for the classes and curriculum can be found at http://ctans.okstate.edu.

core of the IA curriculum consists of six courses, balanced between technical and socio-technical components. The purely technical courses are Applied Information Systems Security, Forensics, and multiple hands-on labs. Courses that cover human and policy issues are Legal and Ethical Issues in Information Technology; and Risk Analysis, Management, and Mitigation. Information Assurance Management deals with control and management issues of both technical aspects as well as human issues.



Supporting the core curriculum is a prerequisite of Computer Competency and Data Networking. The majority of IA students come from the MIS, ECEN, or CS major, which already include these courses; however, other students may still pursue a Minor or Certificate in Information Assurance by taking appropriate prerequisite coursework. The core courses and prerequisites collectively map to all five of the NSTISSI/CNSS certificate standards.



The IA core curriculum has been designed to tightly integrate with any of these three degree programs. Each provides the required prerequisite knowledge, using the terminology and examples from that discipline, complements the IA curriculum with related technology-based courses, and then ties it together with appropriate research, projects, or additional experiences that connect the traditional domain to IA. The goal is to provide the market with top-notch IA technologists, as well as those who understand the application and importance of IA to different types of organizations.

5. **Conclusion**

Information Assurance education is critical to business. As linkages increase between business and consumers, and cross international boundaries, the ability to provide a well-educated and trained workforce to assure the security of information assets becomes a major decision factor for business partnerships. Unfortunately, there is a global shortage in these workers. Out of this shortage has grown academic curricula in IA that are rapidly spreading among the most economically advantaged countries.

Thailand has few, if any, such programs. The country's current economic position and trends, makes the availability of an IA workforce critical to relative advancement within the global marketplace. There already exists a very good technical education structure within the kingdom, as well as many good IT programs.

Information assurance programs have proliferated in some countries, and most institutions will readily share their knowledge about content and development. Thailand can leverage its existing educational offerings with that available content to quickly augment the country's IA workforce. To have the most economic impact on the country, this must occur before further acceleration of the country's information economy. IA is not the driving force for expansion and prosperity, but it is a necessary facilitating tool.

References

[1] Bordogna, J. "Remarks and Introduction of the Honorable Howard A. Schmidt," *AACC/NSF Workshop on the Role of Community Colleges in Cybersecurity Education.* June 26, 2002.

[2] Irvine, C., Chin, S-K., & Frincke, D. "Integrating Security into the Curriculum," *Computer.* 31 (12). 1998. 25-30.

[3] "Worldwide Broadband Survey." http://www.websiteoptimization.com/bw/0601. April 2, 2006.

[4] Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. "2005 CSI/FBI Computer Crime and Security Survey". *Computer Security Institute,* 2005.

[5] Akers, G. "Public-Private Partnership to Protect Critical Infrastructures" *Presented at The Colloquium for Information Systems Security Education*, June 7, 2005.

[6] "Thailand," *The World Factbook*. http://www.cia.gov/cia/publications/factbook/geos/th.html. Updated January 1, 2006. Viewed April 1, 2006.

[7] "The SANS 2005 Information Security Salary & Career Advancement Survey." The SANS Institute, updated January 9, 2006.

[8] "Computing Curricula: Information Technology Volume (Draft)" *IEEE Computing Society / ACM.* April, 2005.

[9] "Security Transcends Technology: About (ISC)^{2,} https://www.isc2.org/cgi-bin/content.cgi?catetory=7. 1 April, 2006.

[10] Valli, C. "Industry Certifications: Challenges for the Conduct of University Security Based Courses," *In the Fourth Australian Information Warfare and Security Conference*. University of South Australia, Adelaide. 2003.

[11] "National IA Education & Training Program," *National Security Agency Central Security Service*. http://www.nsa.gov/ia/academia/cnsstesstandards.cfm, viewed April 1, 2006.

[12] Machonachy, W.V., Schou, C.D., Ragsdale, D., and Welch, D. "A Model for Infrmation Assurance: An Integrated Approach," *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. United States Military Academy, West Point, NY, July 5-6, 2001.