METHODOLOGY FOR CONSIDERING ENVIRONMENTS AND CULTURE IN DEVELOPING INFORMATION SECURITY SYSTEMS

Jeffy Mwakalinga, Stewart Kowalski, and Louise Yngström
Department of Computer and System Sciences,
Stockholm University/Royal Institute of Technology,
164 40, Kista, Sweden
Tel: +468 161 721 Fax: +468 703 9025
jeffy@dsv.su.se, stewart@dsv.su.se, louise@dsv.su.se

ABSTRACT

In this paper we describe a methodology for considering culture of users and environments when developing information security systems. We discuss the problem of how researchers and developers of security for information systems have had difficulties in considering culture of users and environments when they develop information security systems. This has created environments where people serve technology instead of technology serving people. Users have been considered just as any other component in an information system which has resulted in having efficient technical controls but inadequate social controls for security. In this paper we propose a new security framework that considers culture of users and system environments in developing information security systems.

KEY WORDS

Deterrence, response, recovery, value-based chain, adaptability, environments, and detection

1 INTRODUCTION

1.1 Information Systems and Environments

Information systems have to learn to adapt to different system environments and to cultural environments. “A system is here defined as a set of objects together with relationships between the objects and between their attributes related to each other and their environment so to form whole” [22]. An information system can be modelled to consist of abstract systems, (information), living systems (people), and concrete systems (technology) [12]. “Churchman defines environment as those factors which not only are outside the system’s control but which determine in part how the system performs” [22]. An environment of an information system is outside of the control of an information system. There are hostile and friendly environments and an information system must be able to learn and adapt in both the hostile and friendly environments. Who defines the boundary between a system and its environment? What are the factors that set this boundary? Every information system has internal and external environments [22]. We suggest that values of people (culture, traditions, laws, policies, and other social issues) and geographical boundaries need also to be considered when an information systems security designer set the boundary between a system and its environment. Currently with information system designers and developers of IT set the boundary between a system and an environment for users without asking their values. Users of information systems cannot really be regarded as system owners as long as their systems cannot be controlled or defended. The organization has the following environments: labour, customers, ecology, public, material and equipment, land, capital, government, competitors, and technology but an organization controls only part of the environments, as shown in figure 1[22].

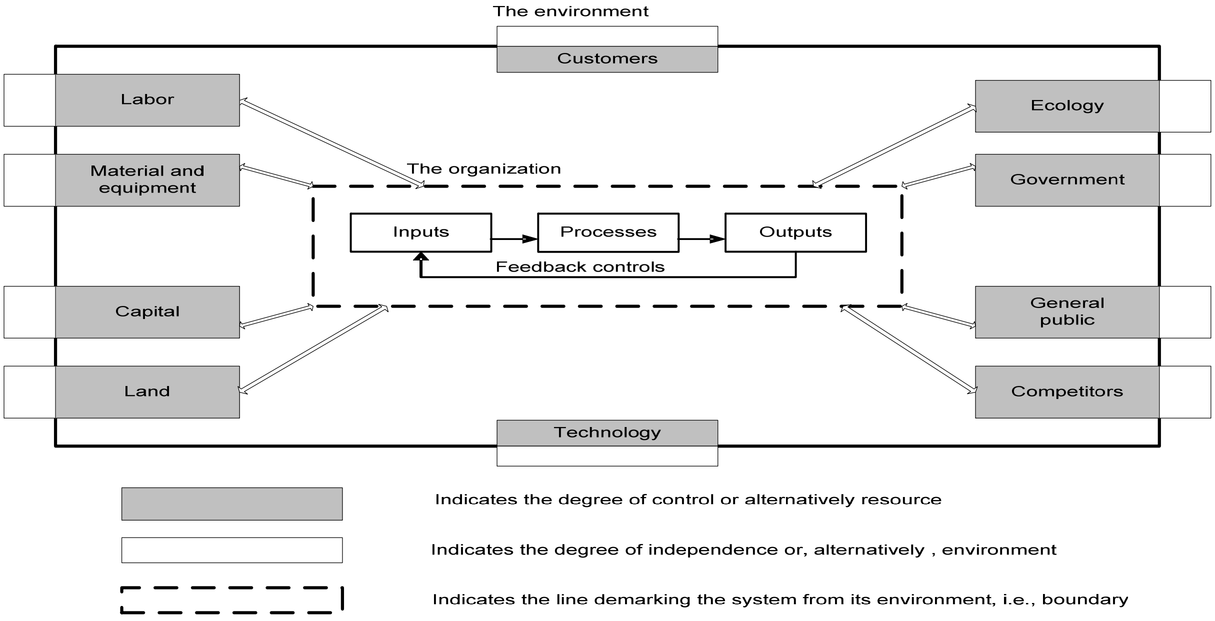

The environment
Customers
Labor
Ecology
Material and equipment
The organization
Government
Inputs
Processes
Outputs
Feedback controls
Capital
General public
Land
Competitors
Technology
Indicates the degree of control or alternatively resource
Indicates the degree of independence or, alternatively , environment
Indicates the line demarking the system from its environment, i.e., boundary

Figure 1: Organization: Its resources and its environment [22]

1.2 Culture and Information Systems

There have been concerns about the role of culture in information systems [20]. Culture has been defined differently by different scholars [10]. Van Dam, Evers and Arts define culture as a set of values, attitudes, and behaviours that people learn or are passed over to them over a period of time

[26]. There is a general agreement among information system researchers that culture affects the way individuals' interact with complex information systems [20]. However, a model has not been developed to measure the effect of culture to individuals. They [20] write,

> "Science educators, from Japan, India and Africa, appear to share a common understanding that science needs to be perceived in a cultural context and to link the development of scientific literacy with an understanding of worldview. Between them, they have examined the faiths, philosophies and logic of students from various cultures to examine, within a culture, the conflict between 'scientific' and traditional concepts of science. Some have been able to link traditional belief and the understanding of scientific concepts or performance of experimental tasks. Others have also shown that science teachers' worldviews and their traditional beliefs affect their teaching and thus their students' learning."

Another question is how much culture affects the decisions that an individual makes when using computer systems [20]. Further concern is whether a function that is provided by an Internet system is consistent across cultures [20]. Van Dam, Evers, Arts did a survey in three different cultures, Moroccan, Surinamese, and Dutch, on user experiences on e-government sites [26]. The results show that Dutch and Surinamese could notice titles on the left side faster while the Moroccan could notice things on the right sides of pages faster. The Moroccans are sensitive to green and red colours. This is because the Moroccans started to read from right to left. Dutch showed a less degree of uncertainty avoidance and they did not read in details but just browsed. The Moroccan needed confirmation that they are performing alright while Dutch and Surinamese did not need this confirmation. The Moroccan culture is a masculine culture in which recognition of achievement is important to participants. Dutch and Surinamese are feminine and they did not need recognition of achievement. Also the Surinamese and Dutch are neutral in culture, which means that showing emotion is regarded as unprofessional. The Moroccan culture is affective which implies that showing of emotion is regarded as normal. The Moroccan is a collectivist culture and it believes that the government website can not have mistakes and so the Moroccans blamed themselves for the mistakes. The Dutch and Surinamese are individualists and they blamed the system for the mistakes. The conclusion was that people with different culture backgrounds experience different problems in using e-government applications.

We have created a new security framework [17] [30] that is based on the Systemic-Holistic approach and the Immune system. The new security framework is a function of the deterrence, protection, detection, response, recovery value-based chain functions. The new security framework applies the system theory and holistic approach to provide security for information. The new security framework applies the principles of the immune system to make systems learn to adapt to environments. We apply the software agents to provide security services in analogy to B-cells and T-cells in immune systems.

2 THE STEPS TO TAKE WHEN CONSIDERING CULTURE OF USERS AND SYSTEM ENVIRONMENTS IN THE NEW SECURITY FRAMEWORK

2.1 Analyze the threat agent

In the first step we start by analyzing the threat agent based on the socio-technical economical system [15]. We document the states that an enemy of an information system could control and the states that an information system owner could control. We created the model of the enemy in which we analyze the methods, tools and processes that an enemy to the systems can apply to attack information systems.

2.2 Classify Assets and perform risk management

The second step is to classify the assets and perform risk management in an information system. We have automated the classification of assets and risk management using software agents. The recovery sub system of the new security framework identifies, assesses, and manages risks. Risk management is based on the Enterprise Risk Management (ERM) – Integrated Framework of the Committee of Sponsoring Organizations of the Tread way Commission (COSO) [21].

2.3 Analyze environments where the systems in focus operate

The third step is to analyze the information system environments in the information system. This involves identifying the local environment, embedded environment, total environment, and predicting future environments [1] [27]. It also involves classifying the environments, analyzing the levels of security of these environments. We identify the environments where a system will be operating. An observation is made over a period of time to study the inputs that are coming and affecting an information system. Then the sources of the inputs have to be studied and traced. Some inputs could be more complicated as they are a result of several environments integrated together. After identifying the inputs, we have to find ways of modifying the inputs so that they do not affect the general state of information system as shown in figure 2. Modification of inputs and outputs is done using the Cybernetics feedback mechanisms [22].There are a number of ways in which we could classify environments [22]. In this work, we choose to classify the environments based on their complexities, dynamism and security levels of environments.

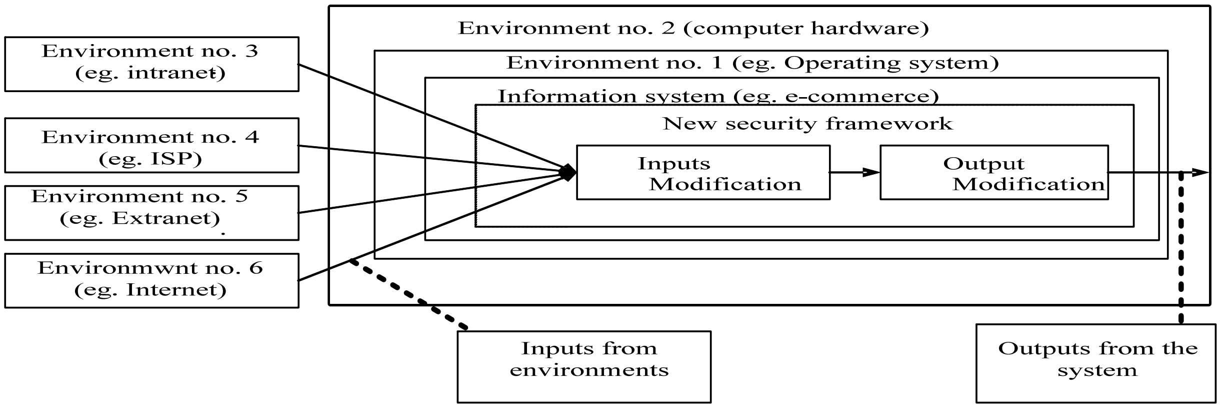

Environment no. 2 (computer hardware)
Environment no. 1 (eg. Operating system)
Information system (eg. e-commerce)
New security framework
Inputs Modification
Output Modification
Environment no. 3 (eg. intranet)
Environment no. 4 (eg. ISP)
Environment no. 5 (eg. Extranet)
Environmwnt no. 6 (eg. Internet)
Inputs from environments
Outputs from the system

Figure 2: Inputs from Environments

An environment could be simple and static, simple and dynamic, static and complex, or dynamic and complex [22]. A static and simple environment has: few factors and components; homogenous factors and components; factors and components that do not change; a stable environment [22]. A complex and static environment has: large number of factors and components; heterogeneous factors and components; factors and components that do not change; unstable environment. The simple and dynamic environment has: few factors and components; similar factors and components; unstable environment; the state of factors and components that change; rate of change of change could be stable or unstable. A complex and dynamic environment has: large number of factors and components; heterogeneous factors and components; high level of uncertainty; unstable environment; the state of factors and components change and the rate of change could be stable or unstable [22]. Examples of environments affecting information systems include an operating system, computer hardware, intranet, Internet Service Provider (ISP), education, hardware, operating systems, electric power, heating, cooling, floods, earthquakes, fire, and cultural environments. What sets the boundary among different environments? Is it policies, ethics, culture, or laws?

The next step is to analyze, using the Systemic-Holistic Approach, the correctness of an environmental systems (like the operating system where an information system is running) at the theoretical/model, design/architecture, and implementation levels [27]. We apply different standards and criteria to analyze the correctness of environmental systems. We analyze the correctness at the different levels because a standard of a system can be correct but its implementation can be wrong. An example of this is the Wired Equivalent Privacy (WEP) encryption system for wireless systems. This encryption system bases on the stream cipher RC4. The algorithm of RC4 does not have flaws but the implementation, the key scheduling and management facilities, is flawed [2]. Many algorithms are basing on wrong mathematical assumptions, which can lead to vulnerabilities in security systems at the higher levels. Then we need to have proofs of correctness at the design and implementation levels.

2.4 Assess the effects of culture and traditions of users to information security

The fifth step is to assess the effects of culture and traditions of users to information security in this information system. We apply the informal cultural model, figure 3, to predict the behaviours of users. Chaula and Yngström made a study in [4], where they examined how human behaviour affects systems security. They found that people with low uncertainty avoidance tend to lack holistic approaches to security which implies that they: lack security in depth measures; "lack attention to details"; tend have "poor risk assessment"; have "poor assumption about motivation, opportunity and methods"; "lack of information classification", use metrics poorly [4]. Cultures where people have low future orientation have ineffective contingency planning. This affects prediction of disasters and preparation if an attack or a disaster was to occur. Cultures where power distance was high result in poor communication on security issues between upper level management and employees and technicians [3] [4]. In low power distance cultures communication and discussion on security issue was better but readiness to report unethical conduct in security was not high [4].

2.4.1 Informal cultural model

We have established an informal cultural model for predicting the behaviour of users to information security system of different cultures. This cultural model will help developers of security for information systems to predict the behaviour and preferences of users of different cultures. This model consists of the following components: General Living System ID; Hofstede; Worldview; Social Identity theory (SIT); Computer Literacy; and General Education as shown in figure 3.

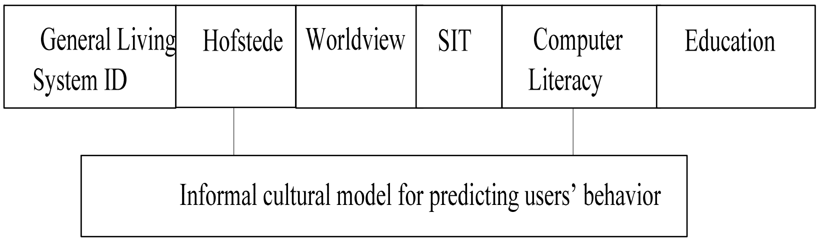


Figure 3: Informal cultural model [17]

The General living System Identity of an individual contains the cell, organ, organism, group, organization, nation, supranational [16] [27]. The general Living identity will provide among others information about cultural background. For instance if the culture reads from right to left then it means the important instructions or pictures in information security have to be placed on the right side of the pages to be noticed faster. The Hofstede [10] component consists of the values: power distance index; individual vs. collectivism index; uncertainty avoidance index; femininity vs. masculinity index; and long-term vs. short-term orientation index. The next component is the Cobern's worldview theory [5] [20]. This theory consists of how an individual understands the world and other people, classification, causality, relationship, self, time and space. This includes a model of the world, what we should do, how we should reach our goals, where are we heading, what is true and false, etc. The next component is the social identity theory with categorization and identification as sub components [23] [20]. These identities can be at personal, group, national, ideological, and religion levels. Then we have computer literacy, which indicates the practical and theoretical computer knowledge that an individual has. The last component is the general education of the individual.

In cultures where power distance is high there is a tendency of over respecting the older people and people who have higher positions in companies. Therefore, there is higher possibility of breaching security if there is external pressure from older people or people with higher positions in a company. This implies that if a boss wanted to borrow a password or a smart card from an employee, the employee is likely to accept the request, thereby breaching security. Therefore, as developers we need to create an authentication system that will not work in cases when there is a possibility of such external pressure to breach security. In countries with low power distance, this possibility is low. There could be a tendency of making security policies and procedures that are not widely accepted by all employees since high-level discussions do not always involve low-income groups in high power distance cultures. Björck and Jiang made a study to compare the implication of culture on IT security between Sweden and Singapore [3]. The power distance in Sweden is low, 31%, while in Singapore it is high, 74% [3] [10]. The manager of a company is Singapore commented that he makes the policies and other issues of IT security and then gives them to the IT department to implement. The Manager of a Swedish company commented on the same issue that he identifies the policies and other IT security issues and then calls a meeting with all the employees involved to discuss and solve the issues.

In cultures that value individualism, people tend to make decisions that are more in an individual's interests than group's interests. This means that a security manager will tend to choose the security decisions of self-interest in the first hand, while security managers from cultures that value collectivism will tend to make security decisions favouring group interests. Another example from the same study [3] is that Sweden scores 71% in the individualism collectivism index, while Singapore scores 20% [10]. It was observed that in Singapore employees consider themselves as an extended family and so they share passwords with each other and they do not consider this as a security breach, while in Sweden people do not share passwords. It was also noted that employees in the Singapore could access even resources that they do not need while in Sweden employees could access only the resources they needed. Hofstede [10] comments that in societies that value collectivism people consider themselves as an extended family, which implies that they trust each other and share responsibilities. This implies in the IT Security world that if for some reasons an employee is not at the workplace now, the employee can ask a colleague to access resources on her behalf by providing all the necessary authentication and authorization credentials. It was also noted that when employees leave companies in Singapore their accounts could remain for a long time without being terminated, while in Sweden when an employee leaves a company for another company the accounts are terminated immediately [3].

In societies where there is the index of uncertainty avoidance is high people tend to be protected against unknown situations and do not always allow their children to experience unknown situations. Students usually expect teachers to have all the answers to their questions [19]. People prefer to have rules, laws and regulations in most areas where environments are structured [19]. In societies where this index is, low people are not protected against unknown situations and they allow children to experience unknown situations. In information systems security people would tend to take more risks and so leave parts of the information systems unsecure.

2.5 Apply Socio-Technical measures where culture and traditions create weak links in information security

The sixth step is to apply social-technical measures [12] where culture and traditions create weak links in information security. Knowledge is applied to understand, to explain, to predict and to control. The informal model will be applied in form of procedures to control. Control can be used to control negatively or positively. The different actions will be assigned values. If the consequence of a certain action or value is negative then this action will be forbidden. If the consequence of a certain value or action is positive then the action will be allowed.

2.6 Provide features to make an information system learn to adapt to environments

In this step we provide measures for making an information system and information security system learn to adapt to environments. Ashby proposed two types of adaptations [25]. The first is to make the system adapt to an environment. The second adaptation is to make the system learn to adapt when the environment changes. We apply the Cybernetics feedback mechanisms [22] and digital immune system [9], variety and regulation [9] and Cybernetic structural models [11] [9] for the first type of adaptation. We apply the Viable System Model, VSM, [9] [1] for the second type of adaptation. Different nations and enterprises apply the VSM [9]. The major application of this model [9] was in Chile during the times of president Salvador Allende. The intelligent forces were trying to destabilize the economy because Allende was a dictator but Chile applied the Viable System Model [30] to stabilize the economy of the country. The environmental disturbances came from the intelligence agencies and the VSM was regulating the disturbances to stabilize the economy [25]. We apply this model to make the security framework learn to adapt to environments. The Viable system model [1] [27] [9], Figure 4, consists of five sub systems: Subsystem 1, Subsystem 2, Subsystem 3, Subsystem 4 and Subsystem 5.

Subsystem no 1 is the lowest level and subsystem 2 is coordinating the operations of subsystem 1 and it receives orders from subsystem 3 [1] [27]. Subsystem 3 is a commanding and controlling subsystem. It controls the internal stability of subsystem 1 and audits it through command and audit channels [27]. Subsystem 4 is concerned with future, adaptation, planning, and simulation measures. Subsystem 4 is responsible for making sure that the whole system learns to adapt to dynamic environments. Subsystem 4 collects data on environmental disturbances and stores them in a database. We apply these data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the system will react to those future disturbances. Subsystem 5 creates rules, identities, goals, and policies of operations. Subsystem 5 monitors the behaviour of subsystems 3 and 4 to make sure that they follow the rules, policies and goals.

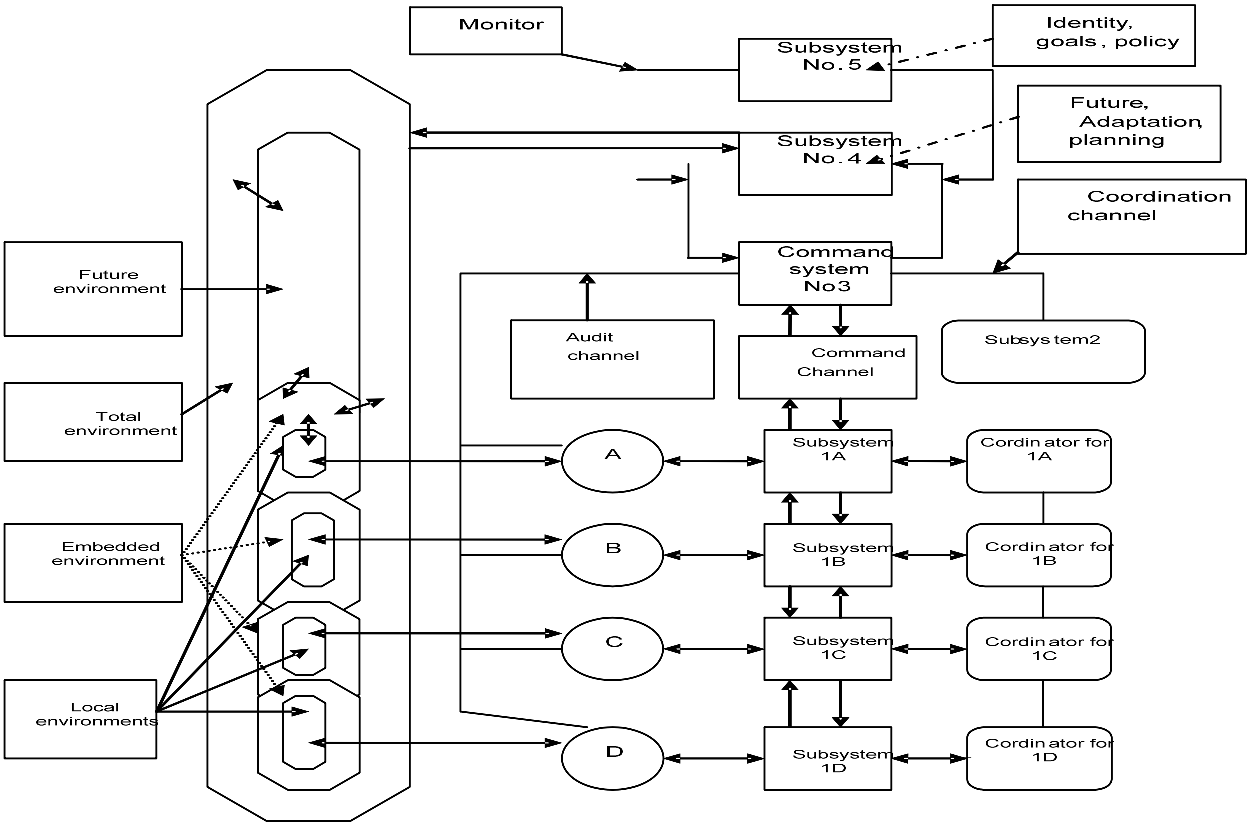


Figure 4: VIABLE SYSTEM MODEL [9]

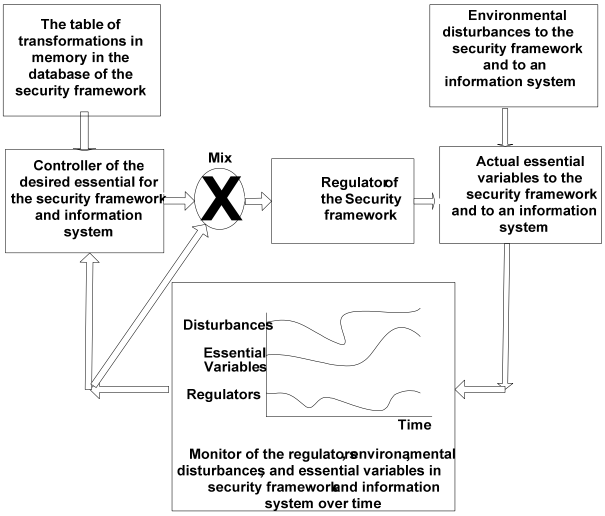
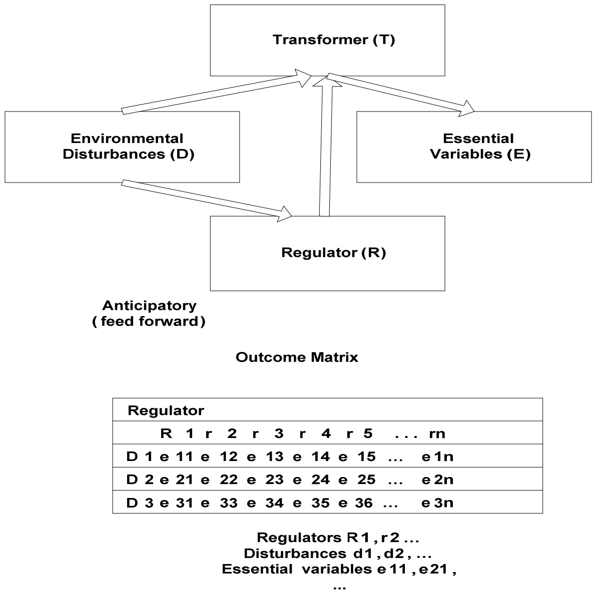

The table of transformations in memory in the database of the security framework
Environmental disturbances to the security framework and to an information system
Controller of the desired essential for the security framework and information system
Mix
X
Regulator of the Security framework
Actual essential variables to the security framework and to an information system
Disturbances
Essential Variables
Regulators
Time
Monitor of the regulators, environmental disturbances, and essential variables in security framework and information system over time

Figure 5: Variety and regulation [9]



Outcome Matrix

Regulator							
	R 1	r 2	r 3	r 4	r 5	. . .	rn
D 1	e 11	e 12	e 13	e 14	e 15	...	e 1n
D 2	e 21	e 22	e 23	e 24	e 25	...	e 2n
D 3	e 31	e 33	e 34	e 35	e 36	...	e 3n

Regulators R 1 , r 2 ...
Disturbances d1 , d2 , ...
Essential variables e 11 , e 21 ,
...

Figure 6: Cybernetic structural model [9]

Every subsystem 1 has a local environment embedded in another environment. This embedded environment is part of a total environment, which contains a future environment. Subsystem 2 is responsible for stabilizing subsystem one. Subsystem 3 monitors the behaviours' of subsystems 1 and 2 and is concerned with internal operational controls of subsystem 1 [9]. It also audits the subsystem 1 to make sure that it performs in accordance to the plans given to it through subsystem 2. Subsystem 4 is concerned with the outside and future of a system. The controller of the desired essential variables mixes them with variables from the monitors to produce the harmless inputs to the information systems. There are two types of feeding: feed forward in which the regulator receives the disturbances and acts before the information security system; in the negative feedback, the information security system receives the environmental disturbances and then the regulator regulates the disturbances via the transformer. For every environmental disturbance, there is a corresponding response as shown in the outcome matrix in Figure 6. The new security framework receives environmental disturbances through the deterrence, detection, prevention, response, recovery sub systems. The adaptability system of the security framework monitors and records the environmental disturbances, essential variables, and regulators over time as shown in figure 5. The adaptability system applies these recorded data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the whole security framework and the information system will react to those future disturbances.

There is a table of transformations in memory of environmental disturbances, essential variables and regulatory disturbances. The controller of the desired essential variables for the security framework and the information system mixes them with variables from the monitors to produce the harmless inputs to the information systems. The implication to information security systems is that the regulator (R) must be able to produce as many responses as the number of disturbances (D) from an environment [9], as shown in Figure 6.

2.7 Compare allocates of economical resources to the different security value-based chain functions

In this step, we do an analysis of how to allocate economical resources to the different security value-based chain functions deterrence, prevention, detection, response, and recovery [13]. In the same way, we analyze to determine how to allocate economical resources to each sub system the new security framework. We have used the Delphi method [28] to construct an ideal security value chain for an information security system in an abstract situation [29] as shown in table 1.

Table 1: Allocation of economical resources on sub systems

Sub system	Deterrence subsystem	Prevention Subsystem	Detection Subsystem	Response subsystem	Recovery Subsystem
Average distribution	18.75%	24.38%	23.13%	14%	19.38%

Analysis of allocation deviation using Chi- square

We analyzed the deviation in allocation of economical resources, shown on table 1, to the security value-based chains using Chi-square [18] $\boldsymbol{X}^2$

$$\chi^2 = \sum_{i=1}^{c} \frac{(O_i - E_i)^2}{E_i}$$

We applied the formula for Chi-square in which Oi is the observed economical allocation on each sub system; Ei is Expected economical allocation on each security value-based function. Ei = 20000. The number of observations, c, is five. We set the degree of freedom to be four. The degree of freedom is the number of observations minus one. The null hypothesis [8] was the deviation from the expected allocation of economical resources to the security value-based chain functions is not significant. We applied the graphpad chi square calculator [7]. The result is that Chi-squared equals 3136.890 with four degrees of freedom. We calculated the probability, P, and found P($\boldsymbol{X}^2$ > 3136.890) = 0.0001. We applied significance level of Probability = 05%. This significance level was established by Fisher [8] who wrote, “The value for P=0.05, or 1 in 20, is 1.96 or nearly 2; it is convenient to take this point as a limit in judging whether a deviation ought to be considered significant or not.” In this observation, we have received the P value to less than 0.0001. This difference is extremely statistically significant. The deviation of the allocation of economical resources to the security value based chain functions deterrence, prevention, detection, recovery, and response from the expected allocation is significant and would indicate that the security culture is different.

2.8 Educate users of information systems in social engineering and about the security framework

The ninth step is to educate users of information systems in the information system in social engineering and about the security framework. This could be done physically, electronically using mobile agents or knowledge bots [24] [14].

2.9 Evaluate the outcomes of the implementation of the new security framework

The last step will be to evaluate continuously the outcomes of the implementation of the new security framework and follow the plan, do, check, act process for continuous security improvement outlined in ISO27001 [6].

3 CONCLUSION AND LIMITATION

We have proposed a new security framework in which we describe a methodology for considering culture of users and environments where information systems operate in developing information security systems. The methodology is also aimed at creating environments where technology serves people instead of people serving technology. We show the importance of applying both socio and technical controls in strengthening weak links that have been created by culture of users. The new security framework provides adaptability features that make information systems learn to adapt to environments. The limitation is that the framework has never been applied in its totality and consequence there is no data to either validate the framework or compare this framework with other information security frameworks.

4 REFERENCES

[1] Beer, S. (1981). *Brain of the Firm*. Great Britain: John Wiley & Sons Ltd.

[2] Bishop, M. (2003). *Computer Security Art and Science*, Addison-Wesley, Boston, USA.

[3] Björck, J., & Jiang, K. W. B. (2006). *Information Security and National Culture Comparison between ERP system security implementations in Singapore and Sweden.* Retrieved November, 2008, from: www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-396.pdf

[4] Chaula A. J. (2006). *A social-Technical Analysis of Information security systems Assurance. A case study for Effective Assurance*, Report 06-016. Doctoral thesis. Computer and Systems Sciences. Stockholm University, Sweden.

[5] Cobern, W. (1991). *The Cultural Nature of the Concept "Scientific Worldview*", Department of Teaching, Learning & Leadership, Western Michigan University, USA. Retrieved January 19, 2009, from: http://www.ouhk .edu.hk/~rcwww/misc/cobern.htm.

[6] ISO 27001 standard, http://27001.denialinfo.com/pdca.htm

[7] Graphpad, (2009). The Chi Square calculator, retrieved February, 2009, from: http://www.graphpad.com/welcome.htm

[8] Fisher, R. A (1926). Statistical Methods and Scientific Inference, New York: Hafner, p 44

[9] Herring, C. E. Jr, (2002). *Viable Software for the Intelligent Control Paradigm for Adaptable and Adaptive Architecture*, Doctoral thesis, University of Queensland, Brisbane, Australia.

[10] Hofstede, G.H., (2001). Culture Consequences: International Differences in Work-related Values, Sage, London.

[11] Howland, D. (1990). *The Cybernetic Modeling of Soviet Systems*, Washington, DC: Defense Intelligence Agency, US Air Force War Defense. Retrieved December, 2008, from: http://www.scribd.com/doc/1486511/US-Air-Force-infowarpre97.

[12] Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Doctoral thesis, Department of Computer Systems Sciences. Stockholm University and Royal Institute of Technology. Stockholm, Sweden.

[13] Kowalski, S., & Edwards, N. (2004). A security and trust framework for a Wireless World: A Cross Issue Approach, *Wireless World Research Forum no. 12,* Toronto, Canada.

[14] Kowalski, S. (2008). Lectures Research in Information systems security. *Scientific methodology course*. Department of Computer systems sciences. University of Stockholm and Royal Institute of Technology Stockholm Sweden.

[15] Kowalski, S., Nohlberg, M. & Mwakalinga, J., (2008). A systemic model for security and risk management in telecom networks. The 12th World Multi-Conference on Systemic, Cybernetics and Informatics: WMSCI 2008, Jointly with The 14th International Conference on Information Systems Analysis and Synthesis: ISAS 2008, June 29th - July 2nd, 2008 – Orlando, Florida, USA.

[16] Miller, J. G. (1978). *Living Systems*, Great Britain: McGraw Hill.

[17] Mwakalinga, J., Yngström, L., & Kowalski, S (2009). A holistic and immune system inspired security framework. Proceedings for the 2009 International Conference on information Security and Privacy (ISP-09), Orlando, FL, USA.

[18] Plackert, R.L. (1983). Karl Pearson and the Chi-Squared Test. International Statistical Review, 51(1), 59-72.

[19] Slay J, (2002). Human activity systems: A theoretical framework for designing learning for multicultural settings. *Educational Technology & Society 5 (1).*

[20] Slay, J., Darzanos, K., Quirchmayr, G., & Koronios, A. (2003). Towards a mature understanding of “culture” in information systems security research. Insights from Research. University of South Australia, School of Computer and Information Science, Mawson Lakes, Australia; Universität Wien, Institut für Informatik und Wirtschaftsinformatik, Austria.

[21] Steinberg, R.M., Everson, M.E.A., Martens,F.J., & Nottingham, L. E. (2004). Enterprise Risk Management (ERM) – Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved February, 2009, from: http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

[22] Schoederbek, P. G., & Kefalas, A., (1990). *Management Systems. Conceptual Considerations*: Boston: Irwin. P 13, 203.

[23] Tajfel, H. (1978). *Differentiation between Social Groups*, Cambridge, UK: Cambridge University Press.

[24] Wallace, R. (2008). *ALICE Artificial Intelligence Foundation*. Retrieved January, 2009, from: http://www.alicebot.org/.

[25] Umpleby, S. A. (2008).*The Viable System Model. Research Program in Social and Organizational Learning*. The George Washington University. Washington DC, USA. Retrieved August 2008, from: http://www.aea-dc.org/resources/2008-8-13-Viable-System-Model-Stuart-Umpleby.doc.

[26] Van Dam, N., Evers, V., Arts, F. (2003). Cultural user experience, issues in e-government: Designing for a Multi-cultural society. Digital Cities 3, University van Amsterdam, Netherlands.

[27] Yngström, L. (1996). *A systemic-Holistic Approach to academic programs in IT Security*, Doctoral thesis, Department of computer system sciences, Stockholm University / Royal Inst. of Technology ISRN SU-KTH/DSV/R--96/21--SE.

[28] Rowe and Wright (1999): The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, Volume 15, Issue 4

[29] Mwakalinga, J. (2009). *Investigating a new security framework based on the principles of the Systemic-Holistic approach and of the immune system.* Doctoral thesis, department of computer system sciences, Stockholm University / The Royal Institute of Technology, Sweden.

[30] Raul, E (2007). Cybersyn: Foundings and convergence between art science and technology in Chile http://www.metaphorum.org/proyecto_cybersyn_ingles.pdf

5 PERMISSIONS

Jeffy Mwakalinga, Stewart Kowalski and Louise Yngström are the authors of this paper. This work is original and does not violate any copyrights, rights and privacy of others. We retain the right all or part of this paper in our future work. We grant the ISSA 2009 organizers the right to publish this paper in the ISSA 2009 proceedings.