https://doi.org/10.48009/1_iis_2016_242-252

Issues in Information Systems
Volume 17, Issue I, pp. 242-252, 2016

FRAMES OF MIND: CULTIVATING KNOWLEDGE AND CYBERSECURITY

Nicole Gong, Robert Morris University, nxgst102@mail.rmu.edu
Guy Philbin, Robert Morris University, philbin@rmu.edu

ABSTRACT

As the size and complexity of cyber threats continue to grow, the protection and management of data, information, and knowledge has become critical to the survival of modern organizations. This paper briefly reviews the history of knowledge management and the evolution of information security through the development of several information security culture frameworks (ISCF). It concludes with a new model illustrating how organizational culture needs to evolve towards a culture of a cybersecurity community of the 21st Century.

Keywords: Cybersecurity, Cybersecurity culture, Knowledge, Knowledge Management, Information Security, Information Security Culture Framework, Information Security Policy

INTRODUCTION

Information and technology are the fabric of our society. As Gleick (2011, p. 298) has observed, a profound shift in frames from energy and matter to information has occurred. This shift has affected our lives, our culture, our science and our technology in profound ways. The capability to manage and secure known and tacit knowledge as a system of information has been crucial throughout human history. "In ancient times," according to Yang Jwing-Ming (1996, pp. 5-6), "it was so important to protect the secret of a style that usually a master would kill a student who had betrayed him, in order to keep the techniques secret. It is no different than a modern government protecting its technology for purposes of national security."

Van Doren (1992, p. xvi) traced long forgotten roots of knowledge from India, Egypt, and Greece; Daikir (2013) begins the history of knowledge management with the Industrial Revolution. We fast forward over the technological and information milestones represented by Babbage's general purpose computing machine, Shannon's mathematical model for communication, Wiener's cybernetics, Turing's Machine, von Neumann's self-replicating machines, Solomonoff's induction theory, and Moore's now famous law to 2016 and the world of Internet and cyberspace.

What has remained constant across this evolutionary trajectory is the need to secure knowledge and protect information. Along the way, the security of knowledge management and information has evolved from closely guarded human access to knowledge stored in martial kata to access control, authentication, and encryption. This paper will briefly review this timeline from the perspectives of knowledge management, information technology, and cybersecurity, examine how various information security frameworks have evolved, and discuss how organizational culture must adapt and defend against threats in today's cyber environment.

Cybersecurity Demands Culture Change

Cyberspace touches every aspect of our lives. It connects people from home, school, work and play. Our nation depends upon the reliability, availability, and security of our critical infrastructure. Executive Order (EO) 13636 "Improving the Critical Infrastructure Cybersecurity" issued February 12, 2013, defined Critical Infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (National Institute of Standards and Technology (NIST), 2014, p. 1). NIST published a draft cybersecurity framework on February 12, 2014, which provides a set of industry standards and best practices to manage cybersecurity risks "…to be updated and improved as industry provides feedback on implementation." (NIST, 2014, p. 1).

At the 6th Annual Billington Cybersecurity Summit, Department of Defense Chief Information Officer Terry Halvorsen indicated that "A change in culture is needed to protect against threats in the rapidly changing cyber domain" (Ferdinando, 2015). Halvorsen highlighted three cyber culture areas that need to be addressed: discipline, economics and enterprise. He added that "Culture is the hardest thing to change." While as yet there is no complete cybersecurity cultural framework, there are many information security culture frameworks (ISCF). The researchers reviewed several ISCFs and divided them into two major groups: policy focused, which emphasize principles of action, and human factors, which emphasize employee behavior. A review of the literature provides a rich set of policy focused and human factors frameworks, however, only one or two cybersecurity culture frameworks (CCF) were found, including NIST's "living document." In order to understand how cybersecurity culture should evolve and what CCFs should address, it is important to investigate how ISCFs evolved.

RESEARCH METHODOLOGY

This paper focuses on how various information security frameworks evolved and asks how cyber security culture differs from information security culture. This study uses a summative approach to flexible qualitative content analysis, which Hsieh & Shannon (2005) describe as "… a widely used qualitative research technique. Rather than being a single method, current applications of content analysis show three distinct approaches: conventional, directed, or summative" (p. 1277). Here are the two operant questions addressed:

RQ 1: How is cybersecurity culture different than information security culture?
RQ 2: How has information security culture evolved?

LITERATURE REVIEW

Knowledge Management (KM) History

The history of knowledge protection is very long; the concept is not new. Although the term "knowledge management" (KM) entered popular usage in the late 1980s when it began to appear in business journals, books, and conference presentations. As Denning (2002) has related, from "time immemorial, the elder, the traditional healer, and the midwife in the village have been the living repositories of distilled experience in the life of the community." Today, however, efficient handling of information and resources within many organizations has focused on knowledge as a valuable commodity embedded in high-tech products and the highly mobile tacit knowledge of employees Dalkir (2013). The following table provides a summary of major points illustrated by researchers.

Table 1: A Brief History of Knowledge Management (KM)

Timeline or Researcher(s)	Important Points or Events
5,000 years ago	Doren's (1992) documented that human thought began 5,000 years ago.
1800s	Industrial Era.
1850 and prior	Focused on "transportation technologies" according to Daikir (2013).
Polanyi (1958) and (1966)	Polanyi's published the book of "Personal Knowledge" and "Tacit Dimension", he started the concept of "Tacit", the ideal was that "we can know more than we can tell."
Drucker (1964)	Drucker coined the term "knowledge worker" (p. 15).
1969	The birth of the Internet.
Engelbart (1978)	Doug Engelbart introduced an early hypertext groupware system that interfaced with other systems. "…Rob Acksyn's and Don McCracken's Knowledge Management System (KMS), an open distributed hypermedia tool, is another notable example and one that predates the World Wide Web by a decade" (Daikir, 2013, p.16).

1980	Thomas (n.d.) noted the appearance of AI systems and systems for managing knowledge. Concepts such as 'knowledge acquisition,' 'knowledge engineering,' 'knowledge-based systems' and 'computer-based ontologies' began appearing.
1989	Daikir (2013) and Thomas (n.d.) agreed that the KM movement started around 1989, with related articles appearing in journals like *Sloan Management Review*, *Organizational Science*, *Harvard Business Review*, and others. Further examples include *The Fifth Discipline* by Peter Senge (1990) and *The Knowledge Value Revolution* written by Sakaiva. "The phrase 'knowledge management' entered the lexicon in earnest" that year, according to Thomas (n.d.). By offering a technological base for managing knowledge, a U.S. consortium formed an initiative for managing knowledge assets.
Senge (1990)	"Focused on the learning organization as one that can learn from past experiences stored in corporate memory systems" (Daikir, 2013, p. 15).
Nonaka and Takeuchi (1991)	Nonaka and Takeuchi (1991) presented a new description of knowledge in an organizational context. It is recognized as "pivotal work." The concept of tacit and explicit dimensions of knowledge was discussed widely in KM circles.
Stewart (1995)	Published "Brainpower" in *Fortune* magazine
Dorothy Barton-Leonard (1995)	Documented case of Chaparral Steel as a KM success story (Daikir, 2013, p. 15).
Nonaka and Takeuchi (1995)	Studied how knowledge is produced, used, and diffused within organizations and how this contributes to the diffusion of innovation.
Kaplan & Norton; A PQC 1996; Edvinsson & Malone 1997, among others	The growing importance of organizational knowledge as a competitive asset was recognized by a number of people who saw value in being able to measure intellectual assets.
Huber (1991), Nonaka (1994), Alvi & Leidner (2001)	Knowledge is defined as a justified belief that increases an entity's capacity for effective action (Huber 1991; Nonaka 1994; Alvi & Leidner, 2001). Knowledge has several perspectives: State of mind, an object, a process, a condition of having access to information, and a capability.
Thomas Davenport and Laurence Prusak (1998)	Approached KM in terms of a marketplace of knowledge.
Alavi and Leidner (2001)	Discussion of knowledge creation, knowledge storage and retrieval, knowledge transfer, and knowledge application. Knowledge creation has four modes: socialization, externalization, internalization and combination.
Denning (2002)	Indicated that "… there is no agreed definition of "knowledge management," even among practitioners. The term is used loosely to refer to a broad collection of organizational practices and approaches related to generating, capturing, disseminating know-how and other content relevant to the organization's business."

Daikir (2013) traced the beginnings of KM to *industrialization* of the 1800s, *transportation* in 1850s, *communications* in 1900s, *computerization* in the 1950s, and *virtualization* in the early 1980s. To these developmental phases in KM history the researchers of this study suggest *cyber-securitization* be added in the late 1990s. C*yber-securitization* refers to the security of the *cybernation*, global digital *informationization* and the ever more frequent use of cyber. First cited by Schneider (1999), cybernation was defined by EO (1997) as "1) the control of an industrial operation or task through processing of information with a computer. 2) A large online community that operates like a nation, or state." *Cyber-securitization* in this study refers to information generated by computers and networks that requires higher security than information security — it is "information security" plus "cyberspace security."

According to Davenport & Cronin (2000, p. 294), "KM is a complex multidimensional concept that requires diverse insights." They point out that KM is used in several domains, including organizational theory, which is how we use it in this paper. While there is debate as to exactly what is meant by KM, most mainstream organizational theorists hew to the notion that KM seeks to create value from knowledge. Because knowledge is difficult to capture and

apply, there is often little or no incentive to share, and because organizational cultures often do not foster knowledge transfer, it is sometimes difficult to realize the goals of KM. Nevertheless, in an ideal word of learning and creative organizations, Nonaka (1991) suggested that a "spiral of knowledge" consisting of both tacit and explicit knowledge is the key to successful KM. Nonaka argues that making tacit knowledge explicit and available to the entire organization — the conversion of human to structural capital — can unify fragmented organizational knowledge and make knowledge transferable. Davenport & Prusak (1998) have approached KM in terms of a marketplace of knowledge. Outside knowledge is often purchased; inside knowledge trades in a different marketplace. Davenport and Prusak suggest the three major currencies for inside knowledge are reciprocity, reputation, and altruism. While there is heathy debate around organizational knowledge creation theory (Nonaka & von Krogh, 2009), it seems fair to say knowledge travels more easily in a creative or learning organization than in many traditional organizations. In either case, knowledge is bought, sold and exchanged within a context of human interaction.

As with cybersecurity, the role of organizational culture plays a critical part in creating, learning, sharing, and managing knowledge. Culture, like tacit knowledge, comes down to individual human beings. No matter the currency, buyers and sellers of knowledge must also share a key human value: trust. Creating and leveraging value from organizational knowledge transactions, like an empowered culture of cybersecurity, is of mutual benefit to all. The term *cybersecurity* was first used by computer scientists to highlight insecurities related to networked computers in the early 1990s. It moved beyond a mere technical conception of computer security when proponents realized that threats arising from digital technologies could have devastating societal effects (Nissenbaum, 2005, p. 63). In this study, *cyber-securitization* represents the best practices of information security culture combined with cyberspace protection culture. This combination creates a cyber security culture.

KM System Security

French (2014) studied fifteen definitions of KM and adopted one created by Kumar et. al. (2006, p. 1): "Knowledge management is an umbrella term for making more efficient use of the human knowledge that exists within an organization.… It is essentially an industry trying to distinguish itself with specialized groupware and business intelligence (BI) products that offer a wide range of solutions. The major focus of knowledge management is to identify and gather content from documents, reports and other sources and to be able to search that content for meaningful relationships." French focused on the security aspect of KM systems, which he argues is defined by three core areas: people, process and products.

Table 2: Knowledge Management System Security

Researchers	Key Points
King, Marks & McCoy, (2002)	KM systems attempt to centralize and electronically capture knowledge; securing that knowledge is key issue in the field of KM.
Awad & Ghaziri (2004)	Security in a KM system relates to authentication, encryption and access control. Knowledge is an important organizational asset.
DeSouza & Vanapalli (2005); French (2014)	Citing DeSouza & Vanapalli (2005), French focused on the security aspects of KM systems, which he argues are defined by three core areas: people, process and products. For an organization to keep a competitive edge, people must have access to appropriate types of knowledge and need to understand when and with whom to share that knowledge. KM products include physical assets such as documents and manuals, as well as electronic KM tools.

KM and Organizational Culture (OC)

Lundy & Cowling (1996) have provided us with the simplest definition of organizational culture (OC) which is: "The way things are done here." Robbins (2001) explained that OC is "the personality of the organization" while Kreitner & Kinicki (1995) describe OC as "…the social glue that binds the members of the organization together." Robbins (2001) indicates that OC represents how people in an organization behave and ptovides the basis of certain activities such as the organization's vision and the behaviors that employees exhibit at different levels. In effect, OC

determines the employees' performance (Knapp, et al. 2009, p. 197; Robbins, 2001). Hofstede, Hofstede, & Minkov (1991) provide a robust description of culture as mental programming: "…in most Western languages *culture* commonly means 'civilization' or 'refinement of mind' and in particular the results of such refinement… *Culture* as mental software, however, corresponds to a much broader user of word that is common among sociologists… *Culture* is a catchword for all those patterns of thinking, feelings, and acting…" (p. 5).

Information Security Culture (ISC) and Information Security Culture Framework (ISCF)

Information security culture frameworks can be grouped into either policy or human factors focused frameworks. Four key frameworks were selected for analysis for this study. Two of them are human factor focused and two are policy focused. The first framework reviewed was STOPE ISCF. According to Al Hogail (2015), "Organizations should focus on employees' behavior to achieve information security, as their security effectively depends upon what employees do or fail to do… Human behavior represents the weakest link in the security chain" (p. 2).

Information security culture (ISC) is defined by Al Hogail & Mirza (2014) as, "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' behavior to preserve information security" (p. 2). Al Hogail (2015) stated that an ISC promoting "security-related human behavior through knowledge, artifacts, values, and assumptions is far more effective than regulations that simply mandate employees' behavior" (p. 2). Al Hogail argues that the enforcement of security policies is less likely to be effective when these factors are ignored. The comprehensive ISCF they proposed is the first reviewed in this study. The Al Hogail and Mirza ISCF consists five dimensions: Strategy, Technology, Organization, People, and Environment (STOPE).

Table 3: The STOPE Information Security Culture Framework

Human Behavior Factors	Scope and Description on (STOPE)	Change Management Tools
Preparedness	Focuses on training and awareness, knowledge acquisition, and change of old practices.	Training, focus group and change agents
Responsibility	Determines employees' practices and performance such as monitoring and control, reward and deterrence, as well as acceptance of responsibility.	Motivation, milestone and measures, involvement
Management	Concerns with security policies, practices, directions, and interaction issues	Management support, resources, and communication
Society and Regulations	Deals with social and cultural aspects and regulation issues.	Culture analysis

The second ISCF reviewed was a three-tier interaction-based framework developed by Da Veiga & Eloff (2010). Tier One is made up of information security components, information security behaviors, and information security Culture. According to Da Veiga & Eloff (2010), the information security components influence and cultivate employee behavior which affects the organization's culture. At Tier Two, the information security components influence individuals, groups, and the organization. Da Veiga and Eloff used an Information Security Policy to explain how the model works. In this example, the organization's policy may state that a laptop must be physically secured at all times. This policy statement provides direction to an employee's behavior as to protecting both the physical asset and the data saved on the laptop. The objective is to "influence the employee's behavior when interacting with the laptop to ensure its safeguarding" (Veiga & Eloff, 2010, p. 199). Tier Three contains seven categories of information security components as defined in previous research by the authors (Veiga, & Eloff, 2010, p. 197). Each category includes a number of information security components. The seven categories are leadership and governance, security management and operation, security policy, security program management, user security management, technology protection and operation and change. An information security component is classified by organizational, group or individual tier with regard to its influence on information security behavior. This classification is based on the main purpose of a component and where it predominantly influences a behavior tier.

The third ISCF reviewed is an information security policy process model created by Knapp, et al. (2009). This data-centric model provides unique value because it was created using data collected from an expert group of 220 Certified Information Systems Security Professionals (CISSP). The researchers conducted a three-phase validation process with a real-world representation of an information security policy process. The following figure illustrates the complete model with ten internal and external influences as well as the broad categories of Information Security Governance and Organizational Information Security. It illustrates that governance is influenced by both environments. For example, the model lists influence categories including regulations, industry standards, and legal requirements, all of which should be considered.

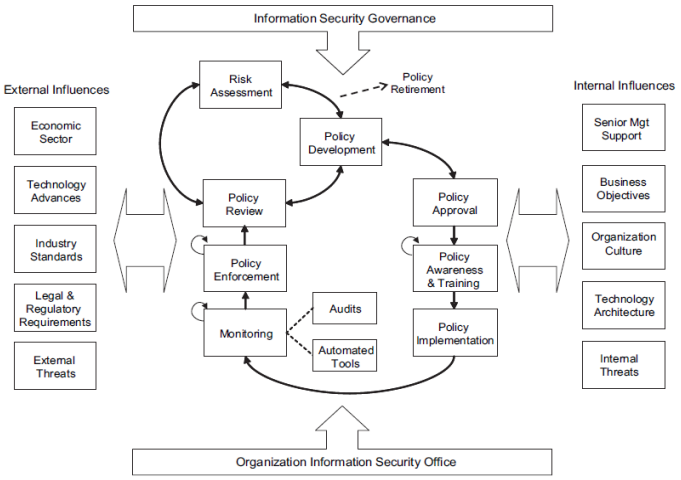

Figure 3. Internal and External Influence Security Policy Process Model, from Knapp, et. al (2009).

The fourth ISCF reviewed was provided by Doherty & Fulford (2006). The essence of this study is not a new framework, but rather why the strategic information systems plan (SISP) should align with the information security policy plan (ISPP). This model stresses the importance of an explicit and careful alignment, "to ensure that the outcomes of strategically important information system initiatives are not compromised by problems with their security" (Doherty & Fulford, 2006, p. 1). A key objective of their ISPP was to "identify opportunities to exploit information;" in this they agreed with Ward & Peppard's (2002, p. 468) statement that the real challenge is "to ensure that information has the highest quality possible, particularly in terms of timeliness, accuracy, completeness, confidence in source, reliability, and appropriateness" (Doherty & Fulford, 2006, p. 55). They specifically called for organizations to use the ISPP for testing "the adequacy of the current information security policy" (Doherty & Fulford, 2006, p. 59). Focusing on roles, responsibilities, and accountabilities, they provided eleven working descriptions of information security policies. Doherty & Fulford (2006) conducted three cases studies to validate their approach. The importance of this study — which is really an example of best practices rather than a framework — is the integration of those two efforts. While the concept of testing securities is good, the examples used for these cases studies are dated and the testing scenarios are not worth repeating.

Cybersecurity Framework

The NIST cybersecurity framework promotes the use of organizational business objectives to guide cybersecurity activities and advocates that organizations consider cybersecurity risk as part of the organizational risk management process. The framework consists of three tiers: the framework core, profile, and the framework implementation. The Core is a set of cybersecurity activities, outcomes and informative references that are common across critical infrastructure sectors. They contain detailed "guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk." (NIST, 2014, p. 1) NIST provides further guidance on how organizations should use frameworks in combination with the existing SP 800-39 which provides recommendations on managing information security risks, from an organization, mission, and information

system point of view. It describes the operational risk management process for federal government agencies, as well as how it can be adopted by private sectors. In addition, it answers questions and provides instructions on how to use it with SP 800-37. Organizations can use the framework and then leverage SP 800-37 to implement the cybersecurity concepts outlined in the framework. Specifically, organizations can leverage the framework core by developing tailored monitoring of security controls.

DISCUSSION

This analysis agrees that people, process, and products are the core of KM security. With respect to people, it appears that constructive knowledge management of employees can improve organizational performance. Various process frameworks have been presented above. The products can be information technology, digital assets, paper documents, databases, information systems, and so on.

The STOPE framework study results indicate that employees are willing to follow an organizational security process and follow procedures to ensure information security. This finding of the STOPE study can contribute to the successful implementation of effective security cultures as it demonstrates a positive relationship between ISC and the application of change management principles. As Hogail (2015) concluded, "change management principles are valuable in creating an effective information security culture."

The quantitative data results of Da Veiga & Eloff's (2010) study validates their framework; the data indicate that there is a positive relationship between employee behavior and organizational culture. An information security culture framework (ISCF) that can assist organizations in implementing security procedures would "cultivate an information security culture that promotes acceptable information security behavior" (Da Veiga & Eloff, 2010, p. 205). This is a culture that disseminates information on desired security behavior, therefore, it would seem that the organization can minimize security risks and maximize business objectives.

The Knapp, et al. (2009) policy process model is comprehensive because it stresses that security governance "is not merely an internal organizational process but can consist of external attributes such as the involvement of a board of directors" (p. 499).

The fourth ISCF model offers an integrated approach with both a strategic and a security policy plan; it promotes best practices, and provides a test and validation process.

Finally, the NIST cybersecurity framework is the most comprehensive. It includes all key points discussed in the four information security frameworks presented here, addresses critical security issues, offers a roadmap to implement the framework, and recognizes the importance of culture. We believe that as cyberspace grows, organizations will need to be more aware of their cyber culture, particularly as to refinements of their virtual organizational culture and employee cyberspace behaviors.

Proposed Cybersecurity Governance Model

As Davenport (1994) succinctly put it: "Knowledge management is the process of capturing, distributing, and effectively using knowledge." While Davenport is most succinct, Duhon (1998) has pointed out that The Gartner Group's definition is most frequently cited: "Knowledge management is a discipline that promotes an integrated approach to identifying, capturing, evaluating, retrieving, and sharing all of an enterprise's information assets. These assets may include databases, documents, policies, procedures, and previously un-captured expertise and experience in individual workers."

In either case, effective knowledge management is the key to success when moving information security towards a culture of cybersecurity. Capturing, sharing, and effectively using knowledge is central to the issues identified in the four ISCF models discussed in this paper. Integrating them into the NIST Cybersecurity framework is what we

propose will provide an excellent governance model moving forward. To put this in more concrete terms, we advocate that organizations capture the knowledge of how an attack happens and predict where risk is greatest, and then act to manage this knowledge by educating and informing people at all four tier levels: individual, group, organization, and community.

Knowledge resides in people, as do cyber awareness, information, and security. The model proposed promotes a cyber culture of sharing, community, and learning. On a macro scale, it would enable government-to-government, government-to-industry, and peer-to-peer industry information sharing. Applying Nonaka & Takeuchi's (1995) organizational knowledge creation theory, community knowledge creation must capture both epistemological and ontological dimensions. On the epistemological side, it would use technology as a tool to capture threat history and document both tacit and explicit knowledge in a community repository. On the ontological side, knowledge would be expanded from the individual, to the team, group, organization and beyond. This is consistent with Nonaka & Takeuchi (1995) who posit that, "A spiral emerges when the interaction between tacit and explicit knowledge is elevated dynamically from a lower ontological level to higher levels" (p. 57). The cyber community model of knowledge we describe here includes knowledge socialization (from tacit to tacit knowledge), externalization (from tacit to explicit knowledge), combination (from explicit to explicit knowledge), and internalization (from explicit to tacit knowledge). Using the proposed cyber culture governance model, organizations would be able to effectively leverage the knowledge in the repository and apply it to their own organizational cyber security governance needs.

Knapp et al. (2009, p. 501) envisioned a corporate governance that accounted for all threats by performing a full risk assessment at the enterprise level to "ensure that information security policies appropriately address diverse threats…" We concur. The Internet changes. Security threats change. Security policies need to change. We would expand this concept to include the cyber community, as cybersecurity should be a community effort. As Swan et. al. (1999) have stated, within the community model knowledge can be tacit and can be transferred through participation in social networks such as occupational or social groups. We believe security threat analysis can be transferred among expert security groups and propose the following Cybersecurity Governance Model which uses collaborative community effort to create a cyber security culture.

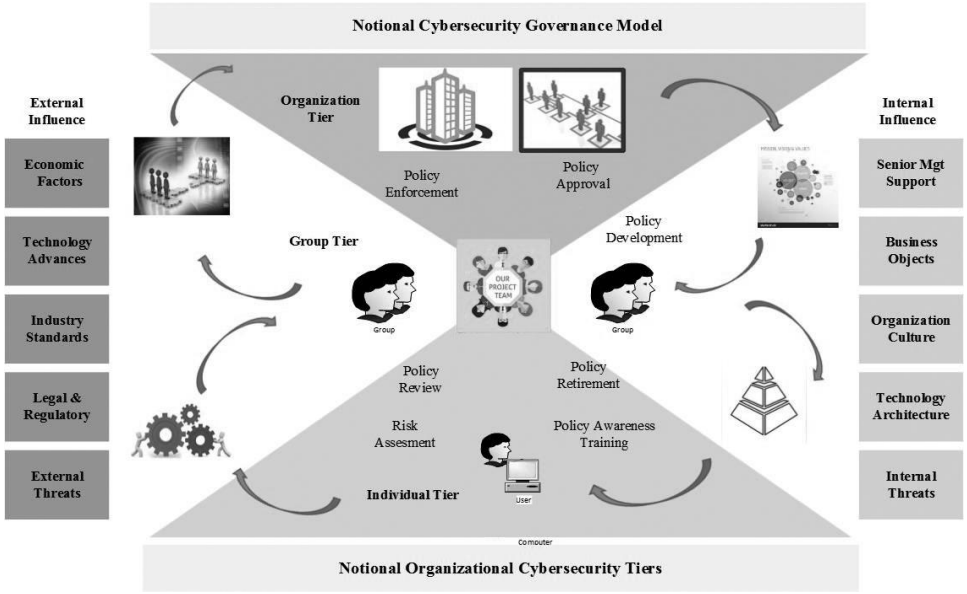

Figure 2**.** Notional Cybersecurity Governance Model

SUMMARY

Cybersecurity and cyber culture are both collaborative community efforts. Cybersecurity should include the five basic dimensions of Strategy, Technology, Organization, People, and Environment (environment in this context includes virtual spaces), a recommended notional governance model based on the NIST cybersecurity framework information flow, and other elements from the Knapp process model. Cyber culture should combine external collaboration with a constructive internal corporate culture, implementing policies that include individual, group, and organizational attributes. Internal cyber culture should rise from individuals to executives, while external cyber culture should assist government and business in shaping a collaborative framework for the cyber community at large. Organizations should maintain a positive relationship between their cybersecurity culture and application of change management principles, ideally with positive activities building cyber culture changes. Organizations should be encouraged to use the NIST cybersecurity framework to develop their own tailored framework and follow the best practices of an integrated KM strategy to test and validate their security policies.

Summarizing briefly, additional community strategy plans and policies are needed. Future investigations should focus on collaboration at the cyber community level, including best practice testing and validation of proposed models. Cybersecurity and cyber culture should become part of a shared community culture.

REFERENCES

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, 107-136.

Al Hogail, A., & Mirza, A. (2014, January). Information security culture: a definition and a literature review. In *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on* (pp. 1-7). IEEE.

Al Hogail, A. (2015). Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. *International Journal of Security and Its Applications,* 9(7), 163-178.

Dalkir, K. (2013). Knowledge management in theory and practice. Routledge.

Davenport, T. (1994). Cited in Koening, M. (2012, May 4). What is KM? Knowledge management explained. Retrieved from http://www.kmworld.com/Articles/Editorial/What-Is-.../What-is-KM-Knowledge-Management-Explained-82405.aspx

Davenport, T. and Prusak, L. (1998). Working knowledge: How organizations manage what they know. Boston, Mass: Harvard Business School Press.

Davenport, E. and Cronin, B (2000). Knowledge management: Semantic drift or conceptual shift? *Journal of Education for Library and Information Science. 451*(4), pp. 294-306.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Da Veiga, A., & Martins, N. (2014). Information security culture. In Academic Conferences and Publishing International Limited.

Denning, S. (2002). How storytelling ignites action in knowledge-era organizations. *RSA Journal*, *149*(5501), 32-34.

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, *25*(1), 55-63.

Executive Office of the President Offfie of Science and Technology policy (1997), *cybernation: The American Infrastructure in the Information Age: A Technical Primer on Risks and Reliability.* Washington DC: Executive Offiec of the President.

Ferdinando, L. (2015). Cybersecurity Demands Culture Change, DoD Official Says. Retrieved April 24, 2016, from http://www.defense.gov/News-Article-View/Article/617767/cybersecurity-demands-culture-change-dod-official-says

French, J. (2014). Keeping the Competitive Edge: Securing Knowledge Management Systems.

Gleick, J. (2011). *The information: A history, a theory, a flood.* New York: Pantheon Books.

Hofstede, G., Hofstede, G. J., & Minkov, M. (1991). *Cultures and organizations: Software of the mind*, *2*, London: McGraw-Hill.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research, 15*(9), 1277-1288.

Jwing-Ming, Y. (1996). *The essence of Shaolin white crane.* Jamaica Plain, MA: YMMA Publication Center. pp. 5-6.

Knapp, K., Marshall, T., Rainer Jr., R., & Ford, F. (2006). Information security: Management's effect on culture and policy. *Information Management and Computer Security,* 14(1), 24-36. doi:10.1108/09685220610648355

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

Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics*, *38*(8).

Nonaka, I. (1991). The Knowledge-Creating Company. *The Harvard Business Review*. pp. 96-104.

Nonaka, I. & Takeuchi, H. (1995). *The knowledge-creating company.* New York: Oxford University Press

Nonaka, I. & von Krogh, G. (2009). Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory. *Organization Science. 20*(3) pp. 635-652.

National Institute for Standards and Technology (2014), NIST Roadmap for Improving Critical Infrastructure Cybersecurity. Retrieved October 10, 2015, from http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

National Institute for Standards and Technology (2013), NIST Framework for Improving Critical Infrastructure Cybersecurity. Retrieved April 25, 2016, from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Polanyi, M. (1958). Personal Knowledge: Towards a Post-Critical Philosophy. University of Chicago Press. ISBN 0-226-67288-3

Polanyi, M. (1966). The tacit dimension. Chicago: The University of Chicago Press.

Schneider, F. B. (Ed.). (1999). *Trust in cyberspace*. National Academies Press.

Senge, P. (1990). The Fifth Discipline. *The Art & Practice of Learning Organization.* New York: Doubleday.

Shannon, C. (1948 July, October). A mathematical theory of communication. The Bell System Technical Journal. 27. Pp. 379-423, 623-656. Retrieved from http://cm.bell-labs.com/mc/ms/what/shannonday/shannon1948.pdf

Solomonoff, R. J. (1964). A formal theory of inductive inference. Part I. *Information and control*, *7*(1), 1-22.

Swan, J., Newell, S., Scarbrough, H. & Hislop, D. (1999). Knowledge management and innovation: Networks and networking. *Journal of Knowledge Management*, 3(4), pp. 262–275.

Turing, A.M. (1950). Computing machinery and intelligence. *Mind*. LIX (236).

Thomas, J. (n.d.). Retrieved April 25, 2016, from http://johnsthomas.wikidot.com/a-brief-history-of-km
Van Doren, C. L. (1992). A History of Knowledge: Past, present, and future. Random House Digital, Inc.

Von Neumann, J., & Oxtoby, J. C. (1988). John von Neumann. *American Mathematical Soc*.

Ward, J., Griffiths, P., & Whitmore, P. (2002). *Strategic planning for information systems, 3*. Chichester: Wiley.

Wiener, N. (1948). *Cybernetics*. Paris: Hermann. pp. 112.