AN INTEGRATED SYSTEMATIC APPROACH TO ORGANIZATIONAL SECURITY

Mahmoud M. Yasin
East Tennessee State University
Andrew J. Czuchry
East Tennessee State University
Michael H. Small
East Tennessee State University

ABSTRACT

As organizations shift from a closed-system model to an open-system model, their security challenges and threats are expected to change from an internal focus to one that must consider the impact of both internal and external forces. To address this change, organizations are encouraged to adopt a more holistic view of organizational security which incorporates physical- and human-asset security, information security, process security, cyber security, and in some instances, national security. The research presented in this paper offers a conceptual framework which advocates incorporating these disparate but interrelated aspects of security into a paradigm of total organizational security.

Keywords: Organizational security, Open system, Rapid assessment methodology, Integrated framework, Competitiveness

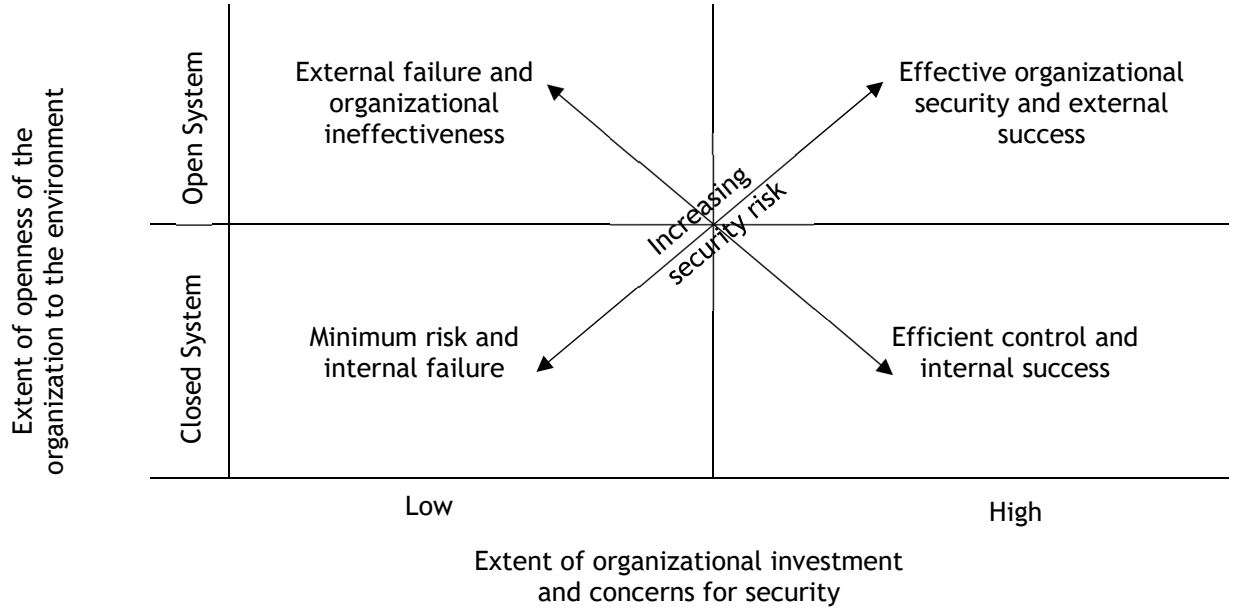
INTRODUCTION

Recent environmental and technological changes and challenges have forced organizations to shift their organizational business model from the closed system orientation to the open system orientation. Such a shift has opened the organization to its customers, its suppliers, and even its competitors. The emerging open system organizational model presented today's organizations with many opportunities and serious

concerns. In this context, the open system facilitated reaching new markets, customers, and suppliers. However, with this openness, different facets of organizational security presented the open system organization with serious threats.

Under the closed system organizational orientation, the focus of organizational security was mainly concerned with internal entities and functions. However, the open system organizational model required the organization to deal with security and risks from a broader perspective. Therefore, organizational security concerns and related investments needed to evolve to keep up with increasing openness of the organization to its environment, customers, and suppliers. Figure 1 depicts the nature of the organizational shift from the closed to the open system orientation in the context of risks, goals, and investments related to organizational security.

FIGURE 1
Extent of Security Investment and Openness of the Organizational Environment



The objective of this research is to present a conceptual framework, which advocates a total organizational security approach. The implementation of such an organizational approach to security utilizes the Rapid Assessment Methodology (RAM). The organizational benefits and challenges resulting from the implementation of the advocated integrated organizational total approach security are addressed.

BACKGROUND

Organizational security can be defined in a variety of ways depending on the particular context and environment in which the organization operates (Brooks, 2010; Hesse & Smith, 2001; Morley & Vogel, 1993). For example, closed-system organizations are likely to focus on intra-organizational security

systems, buttressed by intranets, to control internal sharing of information while protecting and isolating the organization from external security threats (Siegel et al., 1998). Conversely, open-system organizations will emphasize both intra- and inter-organizational security aimed at the effective sharing of internally- and externally- generated information through developing and utilizing intranet, extranet, and internet technologies (Sindhuja & Kunnathur, 2015). This allows for collaboration with external partners, such as suppliers and customers, enabling closer relationships with external constituencies and faster responses to changes in the supply chain. However, open-systems are more exposed to the vagaries of the external environment than closed-systems and are, therefore, likely to be subject to greater internal and external security breaches and other security challenges (McKendrick, 2012; Siegel et al., 1998, Zailani et al., 2015).

ENVIRONMENT

It must be noted, however, that organizational security involves more than just securing the organization's information. Organizations must also secure and protect their buildings and other physical structures, their processes, and any other significant organizational assets. Organizations also need to ensure the safety and security of their personnel (Karlsson et al., 2016). Information security will involve developing, procuring, and securing computer servers, setting up server defenses, such as encryption of data and using firewalls to fend off hacking, malware, and phishing attacks by cyber criminals (Tetri & Vuorinen, 2013; Sbora, 2014; Zhang et al., 2015). Both electronic and physical defense systems, such as electronic surveillance, radio-frequency identification (RFID), metal detectors, and human or robotic guards, can be deployed to protect personnel and physical assets.

Effective security of an organization's information, assets, and people must be coordinated using an organizational security strategy advanced by top management. The distinct security objectives of the strategy must be incorporated into a holistic design of the overall security system, especially its technical and automated components. Organizational security policies should be developed to guide users and evaluators of the various components of the security system to protect these components from unauthorized use and to ensure adequate restraints against voluntarily or involuntarily contravening the security policies (Baskerville & Siponen, 2002). Adequate training on the use of the security systems and details of the security policies should be provided to all designated users (Hwang et al., 2017; Karlsson et al., 2016; Mubarak, 2016; Yuryna, 2017). And such training should be continuously updated to incorporate any changes in the security strategy, the security policies, the configuration of the security systems, or any technological advancements (Abbas, 2011; Tsohou et al., 2015).

Among the various components of organizational security, Information Systems (IS) security has been subject to the most research endeavors. A well-designed IS provides the foundation that allows an organization to focus on information security. Information System security is a complex organizational issue which concerns the implementation of computer technology and supportive technical safeguards, but depends on human interactions to enable the attainment of that security and then contributes to security assurance. Consequently, the success of the IS security system is dependent on human interaction and the extent to which organizational personnel are willing to comply with security policies and guidelines. Human reaction is one area that cannot be designed into IS security systems, but it has the potential to be counterproductive if supporting personnel are not compliant with the security policies. In addition, as

employees become more competent at computer usage, there is an increasing threat of disaffected or disgruntled employees initiating insider threats to the organization (Straub & Nance, 1990; D'Arcy et al., 2009).

It has been suggested that technology, acting on its own, cannot solve the organization's need for information security (Narain Singh et al., 2014; Tang et al., 2016). The human aspect is just as important when an organization must design a secure environment for the organization's information. An employee's attitude to and compliance with organizational security policies can both negatively and positively affect the strength of the information security system. One study indicated that information security knowledge-sharing, collaboration, intervention, and experience all have a significant positive effect on employees' attitude towards compliance with organizational information security policies (Safa et al., 2016). They also suggest that information security is not only intended to protect the information and interest of the organization, but it contributes to the effective protection of the end-users data.

Compared to closed-system organizations, those organizations with an open-systems approach typically require and use more sophisticated information systems including advanced hardware and software. One consequence of the openness offered by the evolving and more advanced information technology has been an increase in the risk of data breaches, thereby increasing the need for improved information security and a heightened emphasis on risk management (McKendrick, 2012). The likelihood that an organization can fall victim to these threats is labelled information systems risk (Straub & Welke, 1998). Information Security is implemented to protect against this risk and is concerned with protecting data and information generated by the business and its partners and also protecting the information system software. Given that a business' data and information can be considered as a vital competitive tool, an organization's Information Security strategy and policies contribute to protection of the business, but can also be considered to contribute to the growth and survival of the organization (Solms & Solms, 2005). Another concern for Information Security is the growing incidence of leaked or stolen information stemming from insider activity (Moore, 2003). The growing incidence of hacking of small and medium sized organizations reported in the 2012 Trustwave Security Report suggests that all organizations should be concerned about information security and develop strategies and policies to deal with potential sources of such attacks.

Organizations must be aware that even though they might have effective security system policies that are well explained to their users, this does not automatically guarantee that the users will follow the policies. Corporate information systems users can pose a threat to the organization's information security systems by accidently or purposefully leaking or destroying classified information. User omissive behavior is defined as the behavior of a user who is not following the corporate security policies, even though the user knows the policies (Hwang et al., 2017; Da Viega, 2016; D'Arcy & Green, 2014). It has been suggested that information systems control can be used as a tool to dissuade users from omissive behavior, but Cox (2012) suggests that much more research is needed to improve our understanding of user's information security behavior, particularly user omissive behavior.

Another type of information security risk is known as insider threat (Chen et al., 2015). Insiders are employees, contractors, consultants, and vendors who can be a target for outsiders or hackers who want to access the organizations sensitive information. There are many theoretical and practical publications explaining how organizations can limit and control insider threats. One of the most common solutions relates to employee awareness training (Taylor & Robinson, 2014; Yoon & Kim, 2013). The main problem

with insider threats is the fact that it is very difficult to identify, monitor, and protect against. Most organizations also tend to focus mainly on outside threats, such as hackers, but it has been found that an important part of preventing hacks or outside threats is by eliminating insider threats. This can be done with the help of Insider Threat Management which focuses on information security and operational risk management to limit threats from trusted insider individuals (Steele & Wargo, 2007).

Process safety and security and cyber security are two interrelated aspects of security that are of particular relevance to larger organizations with open-systems (Gcaza et al., 2017). It is known that an organization's safety climate can vary depending on the industry, but all organizations are highly influenced by their stakeholders' risk behavior. Past studies have examined employees risk behavior to identify triggers that have a negative correlation to risk behavior. Not surprisingly, management commitment to safety, priority of safety, and pressure for production can all have a negative impact on employees risk behavior, increasing the risk of accidents, security breaches, and other undesirable outcomes (Bosak et al., 2013). The term *process security* is concerned with protecting an organization's processes and procedures from terrorist or criminal acts aimed at shutting down processes or converting or diverting the output of the process in a way that is harmful to the organization, its customers, or the environment (Herrmann & Pernul, 1999). For example, process security is breached if a hacker gains access to the process and causes harm to the environment by releasing its hazardous waste in an illegal manner. Process security would seek to ensure that the potential for such attacks on the process is negligible. Solms and Niekerk (2013) assert that cyber security covers all aspects of information security, but also includes the protection of other assets, including humans who can be targets of cyber-attacks but may also unwittingly participate in a cyber-attack. Worldwide terror attacks have also highlighted the importance of national security (Ethala & Seshadri, 2013; Trim, 2005). Cyber-attacks on organizations in the financial sector, major manufacturing facilities, power plants, or government entities often require national security responses (Emerging Cyber Threats Report for 2009).

Advances in process and information technologies have inspired greater collaboration between the functional areas of an organization (Williams & Elliott, 2012). If, for example, a safety problem arises in a manufacturing plant and only the engineering function is involved in addressing the problem's other points of view from, for example, the product development and design function, while the operation function may not be incorporated into the solution. Failing to incorporate these other points of view may risk neglecting the possibility that the safety problem could have been initiated in another department or even from outside the organization. For safety problems that may be precipitated from outside the organization, it is prudent to consider the potential of a cyber-attack and effective process security strategies and policies to minimize such threats ((Homeland Security, 2012). In industries such as the Chemical Sector, or other sectors that create volatile products or generate hazardous waste, organizations should always consider the likely impact and consequences of a cyber-attack on their processes (Gcaza et al., 2017).

In summary, an organization's security system must address internal and external threats and challenges to the organization and should, at minimum, seek to protect the information and processes of the organization while guarding against cyber-attacks and addressing national security issues where necessary. While information technology, including software requirements, are integral to the development of an effective security system, the literature points to various human factors as having great potential to produce threats to the security of the organization. Hence, any effective organizational security system must detail how organizational personnel will be encouraged to form synergistic relationships with

the system with a view to eliminating or minimizing insider threats to the system. The majority of the frameworks developed to measure, improve, or establish higher levels of organizational security necessarily include feedback and continuous improvement to address the fact that the underlying security technologies and internal and external threats are constantly advancing and evolving (Kushwaha, 2016). The challenge is to develop and establish an information security program that is a governance framework that responds to all current and potential future threats and describes: a) what effective organizational security encompasses, b) what are its objectives and policies of the security plan, c) how it relates to the enterprise and its priorities, and d) how it will be integrated into the organization's business goals, objectives, strategies, and activities (ISACA, 2009).

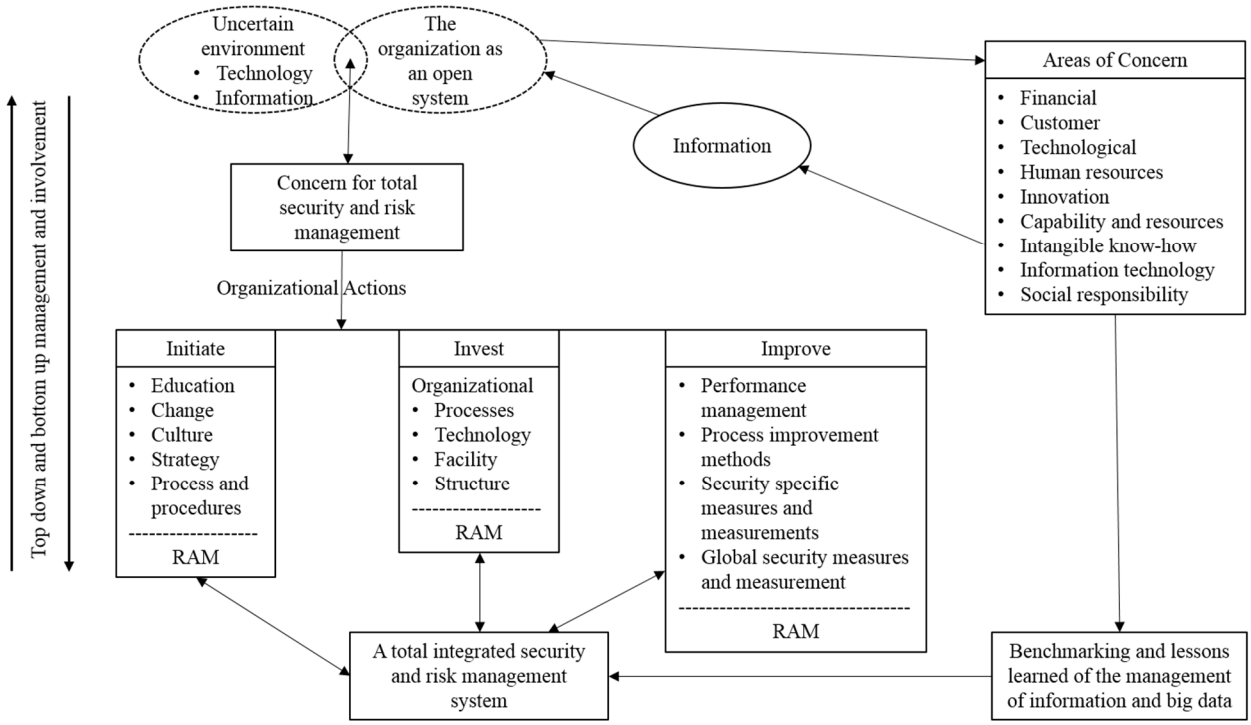
Responding to this challenge, this study proposes a total, systematic, comprehensive, and easy to implement organizational security model. While there are already many models for effecting organizational security, many of them are too complicated, and others focus on one aspect of organizational security making it difficult or impractical to implement for most corporations. The proposed model presents organizational security decision making as a continuous decision-making process. The framework can be utilized to implement a holistic and easily explained organizational security management plan.

PROPOSED FRAMEWORK

Under the closed system organizational model, the emphasis on functional and specific organizational entity security was the norm rather than the exception. As such, organizations invested in different aspects of security. In this context, security efforts and investments were discrete in nature. This often resulted in suboptimization or replication with regard to organizational investment in different aspects related to security.

Recent environmental risks and uncertainties have made the emphasis on security and risk management more relevant than ever before. As such, total and integrated organizational security management systems are beginning to be emphasized, not only by academicians but more importantly by practicing managers. As such, systems are viewed as necessary assets of the modern business organization model. Therefore, security and risk management should not be treated or dealt with discretely, especially in light of the big data environment. The objective of this research is to present a total integrated security system in order to manage the different aspects of organizational security and risks. The conceptual framework in figure 2 advocates a total integrated security organizational approach.

FIGURE 2
An Open System Approach to the Total Management of Organizational Security and Risk



The suggested framework focuses on the different aspects of organizational security which need to be not only managed but also integrated in a form of a complete total security system. The objective of the framework is to enhance organizational security and in the process to minimize organizational risks. Information security, especially in the big data environment, is at the heart of the model. This information and data pertaining to the operational, human capital, customer, and strategic concerns, among other organizational tasks and objectives, are integrated into a total organizational security framework. The proposed framework is systematic and easy to apply. It consists of different stages, such as initiation, investment, and improvement. These stages are aimed at creating a total security integrated approach to all organizational security needs. The goal is to minimize risks related to operations and interactions with the surrounding competitive environment. In this context, the framework views organizations as open systems, which are exposed to the risks and opportunities associated with operating in such an environment.

The Rapid Assessment Methodology (RAM) is used to spark the different stages of the development of the total integrated security system (Yasin et al., 1999; Czuchry & Yasin, 2001; Alavi et al., 2010). As such, RAM provides the decision makers and concerned specialists with quick and immediate answers to relevant questions pertaining to the readiness, potential weaknesses, needed investment, and opportunities for the implementation and improvement for the proposed organizational security system. This, in turn, has the potential to provide the concerned parties in the organization with the motivation needed to secure the investment and human expertise required to complete this process. See Exhibit 1 for a sample of questions, concerns, and weaknesses to be addressed. It is to be noted that the exhibit is provided for

illustrative purposes only. The different areas pertaining to initiation, assessment, investment, and improvement will also have similar questions as provided in the exhibit. Details regarding the mechanics and the procedures associated with RAM can be found among others in the above references.

RAM facilitates the prompt operationalization of the proposed total security approach for the entire organization. In essence, the approach utilized capitalizes on a total involvement of the different members of the organization and relevant partners (see figure 3). This involvement has the potential to increase the sense of ownership and therefore enhance the vested interest in the success of the project. Such involvement encourages both a top down, as well as a bottom up, effort in dealing with and managing critical organizational security concerns (see figure 3). This integrated approach combines the expertise of information management specialists with operational technology experts, while soliciting the support of top management, during the different stages involved.

The total security approach advocated here should serve to govern the actions, tactics, and the strategies needed to afford the organization the security and minimum risk needed to facilitate its operations in an information-based and intensive big data technological environment. In this context, the integration of information technology in the form of software and hardware with analytical models and decision support system is needed in order to ensure the efficient and effective utilization of these needed resources. Such effort is bound to not only promote the security of the organization, but also should assist it in meeting the challenges and opportunities of the competitive open system environments (See figure 4). This, in turn, should be instrumental toward the competitiveness aspirations of the organization.

The security concerns of the closed system organizations mainly focused on internal control of operational information and know-how. However, this concern evolved under the semi open system organizations more toward the management of the selected organizational security concerns, such as information and financial areas. As open system organizations, today's organizations should be concerned with the integration of the different aspects of organizational security. In this context, these organizations are beginning to approach the organizational security strategically. As such, the security strategy should be integrated into the overall organizational strategic planning process. As the organizational security orientation evolved, so did the benefits associated with security investments. These benefits evolved from efficiency to strategic competitive advantage.

EXHIBIT 1
Critical Issues to Address in the Context of Rapid Assessment Methodology for Security and Privacy Risk Mitigation

EVALUATION STATEMENTS	
	Self-Rating Scale
0	**NOT SURE** how our organization compares to this statement.
1	**STRONGLY DISAGREE:** This statement DOES NOT DESCRIBE our company at all. There is no evidence of this activity in our facility.
2	**DISAGREE:** This statement generally DOES NOT DESCRIBE our company. There is little evidence of this activity in our organization.
3	**AGREE:** This statement GENERALLY DESCRIBES our company. There is a great deal of evidence of this activity in our organization.

4	**STRONGLY AGREE:** This statement DEFINITELY DESCRIBES our company. This activity pervades our organization.				
		Circle one			
1.	Our company's leadership, strategic planning, and customer and market focus are directed towards development and/or mitigating information technology security risk.	0	1	2	3	4
2.	Our leaders are effective in setting direction and handling big data analytics with a focus on mitigating information technology security risk.	0	1	2	3	4
3.	When innovation is pushed upward in our supply chain, it is accompanied by a managed process security risk plan.	0	1	2	3	4
4.	When innovation is pulled through our supply chain, it is accompanied by a system-wide security risk mitigation plan.	0	1	2	3	4
5.	Our company is effective in identifying and evaluating qualitative and quantitative global business information and has a well-defined approach to intelligent security risk mitigation.	0	1	2	3	4
6.	Our company is effective in determining current and future requirements, needs, and expectations of customers in current and/or potential international markets and has a well-deployed security risk management system.	0	1	2	3	4
7.	We offer mobile services through the global market place and our mobile services are protected by encryption technology.	0	1	2	3	4
8.	We have a fully integrated B-2-B e-commerce system that is protected by a strong security mitigation system.	0	1	2	3	4
9.	Baldridge and/or European quality criteria are augmented with security risk criteria.	0	1	2	3	4
10.	We have a fully integrated ERP system throughout our supply chain accompanied by an appropriate security program risk management system.	0	1	2	3	4
11.	Information Technology security policies and procedures are extensive and fully deployed; and security risks have been prioritized with mitigation plans fully deployed for high and medium risk areas.	0	1	2	3	4

FIGURE 3
An Organizational Team Approach to an Active Integrated Total Organizational Security Effort

Organizational Entity	Action and Accountability
Top Management	Initial, committee resources, champion for sustainability
Management Information Department	Manage the operations of information related functions
Operations Department	Translate operational details into workable nontechnical secured operations
Engineering and RD	Minimize the accessibility of know-how and breakthrough information
Accounting Department	Create accounting method to move security or lack of
Market Department	Information customers, but did not leave trace to supply-chain and sources of raw material. Integrate these efforts with operation department
Employee	• Security is every person's business • Motivation for loyalty and security
Customers	Encourage reporting critical incidents
The Security Team Membership	• Representatives of all entities • Accounting • Rewards • Identify problems before they happen
The Organization	Promote • Innovation, risk taking • Relaxed environment but maintain an eye of security

FIGURE 4
Competiveness Through the Implementation of an Integrated Security Organizational Approach: An Open System Orientation

Benefit:	Efficiency	Effectiveness	Strategic Competiveness	
Risk of Security Breach: Open System			Public information Marketing Image, Products, & brands Web site publicity and sales information on products and service Human resources hiring information	High
Risk of Security Breach: Semi Open System		Supplier requirements, specifications, pricing & logistics information Human resources employee general information SEC required information for publicly traded companies Sustainability Innovation Map ITIL and Baldridge into these categories as a basis for RMAs		Medium
Risk of Security Breach: Closed System	Intellectual Property & Trade Secrets Customer Identity Social Security + Credit Card information Manufacturing plant control; robotics, safety, delivery Human resources individual sensitive information: Security + Credit Cards Financial specifics on pricing, bank notes, and covenants		Plant floor controls MRP data	Low
	Low	Medium	High	
Organizational Security Orientation	**Control**	**Management**	**Strategy**	

Impact of Security Breach

Benefits of Openness

Based on the material presented in this research, management of today's organizations is called upon to utilize a staircase approach, as it attempts to ensure the achievement of the integrated organizational security system. Toward that worthy end, the following steps are in order.

First, a complete assessment of the current status and practices of the different facets of organizational security should be conducted. This step is carried out through the systematic utilization of the Rapid Assessment Methodology alluded to earlier.

The second stage attempts to uncover the security gaps related to tasks, systems, and processes throughout the organization.

The third stage involves securing the investment needed to close the identified security gaps. It is to be noted that such investment may be multifaceted in nature, as it not only focuses on the financial resources needed but also on the required human expertise, procedural changes, and perhaps process reengineering.

Fourth, modifying the existing organizational culture in order to promote a total organizational security approach. This might require the elimination and/or modification of current practices and procedures. In addition, a clear path of responsibility and accountability must be documented and communicated to all members of the organization.

The final stage includes the integration of the needed policies, software, hardware, and proper training for the chief security officer and concerned employees.

The newly founded total organizational security approach should be monitored through a rigorous continuous improvement effort in order to ensure the quality of the different facets of the organizational security approach. This effort should be an ongoing process, which utilizes well defined measures.

A total organizational security approach is not only needed, but rather it is becoming a necessity in the road toward sustainability and competitiveness. In this final analysis, organizational security is a required prerequisite to strategic advantage and overall competitiveness.

CONCLUSIONS AND IMPLICATIONS

While closed system organizations were concerned mainly with efficiency, open system organizations are concerned with both efficiency and effectiveness. Effectiveness requires the organization to open its system to customers, suppliers, and other entities in the environment. This leaves the organization open to serious risks and potential security threats. The framework advocated in this study represents an organizational-wide effort to deal with such threats, while still benefiting from the openness to its customers and suppliers. The framework is conceptual and integrated in nature. However, it can be implemented using the Rapid Assessment Methodology (RAM) in a rather short period of time. This process could be accomplished with limited organizational investment. The success of this immediate yet affordable implementation should motivate the management of the organization and give it the justification needed for implementing the integrated security approach and related system. In essence, RAM can spark the organizational effort and invest toward a total organizational security system. In this context, obtaining quick results should energize the entire organization for completing this very worthy project. In today's business environment, organizational security is essential to competitiveness. This is especially true in a global competitiveness arena where the success or failure of the organization may be directly associated with its ability to maintain a secured reputation in the market.

REFERENCES

Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. ***I****nformation Management & Computer Security*, 19(1), 5-24.

Alavi, J., Yasin, M., Koubida, S., & Small, M. (2010). Moroccan tourism realities and potential: A rapid assessment methodology approach and a framework for future improvements. *Journal of International Business Research and Practice*, 4(1), 65-75.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5), 337-346.

Bosak, J., Coetsee, W., & Cullinane, S. (2013). Safety climate dimensions as predictors for risk behavior. *Accident Analysis & Prevention*, 55, 256-264.

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. *Security Journal,* 23(3), 225-239.

Chemical Sector Coordinating Council in partnership with the U.S. Department of
Homeland Security (2012) Securing Industrial Control Systems in the Chemical Sector ROADMAP

AWARENESS INITIATIVE – A CASE FOR ACTION. Retrieved from https://www.dhs.gov/sites/default/files/publications/Case-for-Action-Sept-2012-508_0.pdf.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, 55(3), 11-19.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior,* 28(5), 1849-1858.

Czuchry, A., & Yasin, M. (2001). Enhancing global competitiveness of small and mid-sized firms: A rapid assessment methodology approach. *Advances in Competitiveness Research*, 9(1), 87-99.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474-489.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information and Computer Security*, 24(2), 139-151.

Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Center, October 15, 2008. Retrieved from: https://smartech.gatech.edu/handle/1853/26301.

Ethala, K., & Seshadri, R. (2013). Combating cyber terrorism-assessment of log for malicious signatures. *American Journal of Applied Sciences,* 10(12), 1660-1666.

Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security*, 25(3), 259-278.

Herrmann, G., & Pernul, G. (1999). Viewing business-process security from different perspectives. *International Journal of Electronic Commerce*, 3(3), 89-103.

Hesse, L., & Smith, C. L. (2001). Core curriculum in security science. In H. Armstrong (Ed.), *Proceedings of the 5th Australian Security Research Symposium. Perth, Western Australia: School of Computing and Information Science*, Edith Cowan University, 87-104.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, 41(1), 2-18.

ISACA. An introduction to the business model for information security (2009). ISACA 1-28. Retrieved from http://www.isaca.org/Knowledge Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information and Computer Security*, 24(5), 418-451.

Kushwaha, P. (2016). Amalgamation of the information security management system with business – paradigm shift. *International Journal of Computer Science and Information Security*, 14(1), 105-112.

McKendric, J. (2012). Closing the security gap – 2012 IOUG enterprise data security survey. *Division of Information Today*, 1-37.

Moore, M. M. (2003). Employee security education: Pillars of your community. Retrieved from www.csoonline.com/article/217810.

Morley, H. N. & Vogel, R. E. (1993). The higher education dilemma for the private security professional: Delivery methodologies and core curriculum from the practitioner's perspective. *Security Journal*, 4(3), 122-127.

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication and Ethics in Society*, 14(3), 254-271.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, 27(5), 644-667.

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Sbora, C. (2014). Indicators for determining collaborative security level in organizational environments. *Informatica Economica*, 18(4), 131-143.

Sindhuja, P. N., & Kunnathur, A. S. (2015). Information security in supply chains: A management control perspective. *Information and Computer Security*, 23(5), 476-496.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Solms, B. V., & Solms, R. V. (2005). From information security to…business security? *Computers & Security*, 24(4), 271-273.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security*, 16(1), 23-33.

Straub, D. W., & Nance, R.J., (1990). Coping with systematic risk: Security planning models for management decisions making. *MIS Quarterly,* 22(4), 441-469.

Straub, D. W., & Welke, R. J. (1998). Coping with systematic risk: Security planning models for management decisions making. *MIS Quarterly,* 22(4), 441-469.

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, 17(2), 179-186.

Taylor, R. G., & Robinson, S. L. (2014). The roles of positive and negative exemplars in information security strategy. *Academy of Information and Management Sciences Journal*, 17(2), 57-79.

Trim, P. R. J. (2005). Managing computer security issues: Preventing and limiting future threats and disasters. *Disaster Prevention and Management*, 14(4), 493-505.

Trustwave Global Security Report 2012. Retrieved from https://www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 24(1), 38-58.

Williams, G., & Elliott, S. J. (2012). Combining functional safety and cyber security. Control Engineering, 59(11) 32.

Yasin, M., Czuchry, A., Jennings, D., & York, C. (1999). Managing the quality effort in a health care setting: An application. Health Care Management Review, 24(1), 45-56.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People*, 26(4), 401-419.

Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information and Computer Security*, 25(2), 118-136.

Zailani, S. H., Seva Subaramaniam, K., Iranmanesh, M., & Shaharudin, M. R. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy. *International Journal of Physical Distribution & Logistics Management*, 45(7), 652-673.

Mahmoud M. Yasin (mmyasin@etsu.edu) is Professor of Management at East Tennessee State University, P.O. Box 70625 Johnson City, Tennessee 37614.

Andrew J. Czuchry (czuchry@etsu.edu) is the AFG Industries Chair of Excellence in Business and Technology and Professor of Management and Engineering Technology at East Tennessee State University, P.O. Box 70619, Johnson City, Tennessee 37614.

Michael H. Small (smallm@etsu.edu) is Professor of Management at East Tennessee State University, P.O. Box 70625 Johnson City, Tennessee 37614.