Issues in Information Systems
Volume 17, Issue IV, pp. 227-236, 2016

ARCHITECTING A CYBERSECURITY MANGEMENT FRAMEWORK

***Susan M. Tisdale, Robert Morris University*, smtst173@mail.rmu.edu**

ABSTRACT

There are a lack of holistic cybersecurity management frameworks. This qualitative study used a systems and complexity approach to identify business, socioeconomic, and information technology (IT) cybersecurity factors, and their interrelationships. The study examined IT management frameworks and cybersecurity standards and literature. Interviews and a focus group of subject matter experts followed. The research found cybersecurity is a leadership, not a technical issue. Cybersecurity is an ecosystem; its components are interrelated and inseparable, requiring qualitative, subjective, and risk interventions. Cybersecurity, IT, and threats are too complex and volatile for organizations to manage all risks and vulnerabilities in a timely, agile manner. Companies must take off-line, segregate and encrypt their most sensitive information and curb their appetites for new, unsecured technology. Cybersecurity is multilayered, requiring subspecialists, who often serve conflicting business needs and security objectives. Organizations need to raise cybersecurity to a business level function, not subordinate to IT, and involve cyber specialists at all levels and phases in the business lifecycle. Cross-pollinating employees, especially from finance, cybersecurity, and IT, increases awareness of the others' requirements and facilitates more rapid portfolio, lifecycle cybersecurity interventions. Finally, the study of cybersecurity management requires agile, qualitative, multidisciplinary methodology to produce thick, quick, actionable information.

Keywords: Cybersecurity Management, Socioeconomics, Information Technology, Risk Management

INTRODUCTION

Despite advancements in technology, countermeasures, and situational awareness, cyber breaches continue to increase in number, complexity, and severity. In June of 2015, the U.S. Office of Personnel Management (OPM) discovered that millions of records containing federal employees' and contractors' security clearance information were stolen (OPM, 2015). Healthcare data are particularly vulnerable. Cyber breaches in this industry increased 125% from 2010 to 2015 (Ponemon Institute, 2015). This was attributed to the amount of personal information contained in these records and that healthcare providers, employers, pharmacies, and insurance companies do not have the resources to protect the information (Ponemon Institute, 2015). The RAND Corporation reported the black market for hacking tools were, "more profitable than the illegal drug trade" (Ablon, Libicki, & Golay, 2014, p.11). These tools are easy to use and law enforcement was finding it difficult to infiltrate these groups as these groups are sophisticated in screening those who use their services (Ablon, Libicki, & Golay, 2014). Unfortunately, research has found little empirical evidence linking effective governance with reducing the impact of cyber incidents on business objectives (Flores & Farnian, 2011).

To improve an organization's cybersecurity posture, research suggests a more holistic approach is needed. Cybersecurity framewords are fragmented and vary in effectiveness (Atoum, Otoom, & Abu Ali, 2014). Cybersecurity decisions should be driven by business objectives, laws and regulations, the information that must be protected, and security threats (Jirasek, 2012). Security is in every IT activity and those activities need to match business requirements (Bunker, 2012). Most technical cybersecurity solutions failed to consider cost, operational tradeoffs, and the ability of adversaries to adapt to vulnerabilities (Hughes & Cybenko, 2013). Cybersecurity is also interdisciplinary and considers economics, technology, usability, and psychology (Julisch, 2013).

Problem and Purpose

The problem is that there are multiple different business, socioeconomic, and IT perspectives on cybersecurity management. The purpose of this study was to identify a comprehensive, holistic, set of cybersecurity management factors, and the interrelationships of those factors. To address the complexity, interrelationships, and interaction of

the multiple stakeholders and factors involved in cybersecurity, four research questions were used: (a) What are the business components associated with cybersecurity management? (b) What are the socioeconomic components associated with cybersecurity management? (c) What are the IT components associated with cybersecurity management? and, (d) What are the interrelationships of the socioeconomic, business, and IT components associated with cybersecurity management?

RESEARCH METHODOLOGY

Data Collection and Analysis

Data collection and analysis followed three stages using Spradley's (1979) guidance on domain, taxonomic, and thematic analysis. Domain analysis was used to identify the business, socioeconomic and IT domains. The taxonomic analysis further developed the domains and subdomains and the thematic analysis captured the relationships between and among the domains and subdomains. A content analysis followed by in-depth interviews and a focus group comprised the data collection. In Stage 1, multiple sources were used to examine and develop the cybersecurity management domains and subdomains. The information gained from the content analysis also informed the development of questions used for the in-depth interviews and focus group. In Stage 2, 19 in-depth interviews were used to refine the domains and subdomains and develop the interrelationships of the people and data within and among the domains and subdomains. The information from this activity was also used to develop an initial cybersecurity management framework. In Stage 3, a focus group, comprised of 5 participants from the in-depth interview group, refined and validated the framework and further examined the interrelationships.

Participants

The participants were chosen based on their respective fields of experience within the business, socioeconomic or IT domains and their experience with cybersecurity. All participants had at least 20 years of experience. The focus group was comprised five of the in-depth interview participants. They were selected based on their cybersecurity experience and to get a diverse sample from each of the domains. Table 1 summarizes participant demographics. Each interview was scheduled for 30 minutes but most went from 45 minutes to one and one half hours. The focus group met for one hour. The interviews and focus group discussions were recorded, and transcribed verbatim.

Table 1. Summary Participant Demographics

Summary of Participant Demographics	
1: Data Analyst, 30 years' experience	11: Business Continuity Manager, 25 years' experience
2: Enterprise Architect, 25 years' experience	12: Contacting Officer, 25 years' experience
3: Systems (Interdisciplinary) Engineer, 30 years' experience	13: Computer Science Professor, 25 years' experience
4 Cost Estimator, 37 years' experience	14: Test and Evaluation Engineer, Professor, & CEO, 35 years' experience
5: Chief Financial Officer, 25 years' experience	15: Cyber Human Resource Manager, 35 years' experience
6: Computer Systems Engineer, 30 years' experience	16: Program Manager, 20 years' experience
7: Data Analyst, 20 years' experience	17: Attorney, 30 years' experience
8: Chief Information Officer, 25 years' experience	18: Actuary & Systems (Interdisciplinary) Engineer, 20 years' experience
9: Federal Law Enforcement Agent, 20 years' experience	19: Systems (Interdisciplinary), 25 years' experience
10: Chief Information Officer, 25 years' experience	

Instrumentation

The instrument used for the in-depth interviews and focus group was open-ended, semi-structured questions. The questions were field tested prior to use. The same data analysis code book was used during all stages of this research. The code book was based on the Clinger-Cohen Act Core Competencies (2012), which discuss business, socioeconomic, and technology factors associated with IT management. These factors were modified to address cybersecurity. For intercoder reliability, the code book was provided to two individuals to examine how the Clinger-Cohen Core Competencies for IT management paralleled the proposed cybersecurity management domains and subdomains. This examination yielded an approval rating of 98%.

Cross Validation

Each of the cybersecurity domains and subdomains are complex disciplines in themselves. Reviewing all or most of the relevant material was impossible, given the timeline of this research project and the rapid publication and turnover of cybersecurity related information. Thus, only major standards and regulations were reviewed, such as the U.S. Department of Commerce's National Institute of Science and Technology's (NIST) Risk Management Framework (RMF) (2014) and Federal Information Processing Standards (FIPs) (2006); the U.S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM) (2015); Control Objectives for Information and Related Technology (COBIT) (2015); and, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Security Standard, ISO/IEC 27001 (2013). A decision was made to limit the literature review to peer and academic research, papers, and conference proceedings although a great deal of good cybersecurity information is published by trade organizations and consultants. Primary consideration was given to literature less than five years old. However, in many cases, literature older than five years was used, particularly in cases where information in certain subdomains experienced spurts of research or where the concepts were still valid (e.g. economic models).

RESULTS

This study is significant in that there are few holistic studies on cybersecurity management. The study's key findings show how cybersecurity continues to grow in complexity and uncertainty despite advances in technology and increased attention to cyber matters. Changes occur at a blistering pace, making it difficult, if not impossible, for companies, law makers, academia, and professional organizations to respond in a timely manner. It was the qualitative approach to this research that developed the thick, rich detail and context which revealed critical, non-substantive elements as the keys to managing cybersecurity, not the technologies themselves. Overall, a framework that considers business, socioeconomic and technology factors provided a comprehensive, holistic approach to cybersecurity management. Business components specifically address cybersecurity in an organization's governance and policy, investment planning and control procedures, resource strategy and planning, and enterprise architecture. Socioeconomic components address cybersecurity in the organization's leadership and human capital management practices, process and change managegment, knowledge management, risk management, and economic models. The technology components detail cybersecurity assessment and performance requirements; cybersecurity requriements in programs and project management; and, specific cybersecurity policies, tactics, tools, techniques and procedures.

Cybersecurity is a Leadership and Qualitative Issue

All participants in the focus group agreed that cybersecurity was a leadership and qualitative issue. Cybersecurity is an ecosystem. It is complex and multi-disciplinary and cannot be separated from other business functions. Cybersecurity is different from IT and must be elevated to a business level function. Business, IT, and cybersecurity objectives and requirements often conflict, requiring the senior leaders to take an active role in understanding cyber needs, prioritizing objectives, taking responsibility, and making the security decisions. Moreover, cybersecurity is about controlling an organization and a person's appetite for new, unsecured technology. So long as this appetite exists, and those capabilities are being rushed to market without adequate security, systems will be vulnerable.

Cybersecurity Critical Success Factors

Critical Success Factors are used in business to describe those elements that an organization must master to succeed. Although this research was not structured to specifically identify and evaluate cybersecurity critical success factors, several issues emerged that merit further exploration. These were the tangible and intangible elements about which study participants were passionate. Many of these factors, summarized and characterized in Table 2, are intangible by nature and are the hardest, but most critical, to identify and address. The table is divided into two columns. The first column lists the critical success factor. The second includes a description of the key attributes and a brief discussion of the issues.

Table 2. Critical Success Factors

Cybersecurity Critical Success Factors	
Critical Success Factor	**Issues and Attributes**
Effective Organizational Interpersonal Relationships	Cybersecurity requires multidisciplinary teams. Each business function must understand the others' information needs, cyber risks, and impact from breaches. Cyber professionals must understand business objectives and communicate cyber issues to stakeholders in a manner they understand. Cross-pollinating people, especially from finance, cyber, and IT departments, increases awareness of the other's roles and responsibilities. Co-locating personnel, especially for intrusion detectors and responders, decreases the time to address issues.
Mastery of Agility	Threats, risks, and guidance continually change. Detecting, reacting, and responding to threats oftentimes requires immediate action across the organization.
Effective Organizational Cognition	As long as organizations have an appetite for new, unsecured technologies, security will be an issue. Organizations must balance the tension between wanting on-demand information with what is important and what to secure.
Effective Individual and Group Cognition	Cybersecurity is intangible and difficult for some people to understand. People become saturated with too many cyber alerts, thus ignoring threats. The organization must balance the dissemination of information with over saturation.
Effective Transference of Knowledge	The individual remains the weakest link in cybersecurity. Effective knowledge management and training is essential. Younger generations (digital natives) learn differently from older generations (digital immigrants). Training must adapt to different learning styles and needs. An organization needs to use innovative and agile methods to identify data, analyze the data and transfer knowledge for actionable information. A dedicated, multi-skilled person or team is needed to manage cyber information and associated processes.
Effective Governance	Governance is not one-size fits all and as forced communication, does not work.
Common Lexicon	Cybersecurity taxonomies and lexicons lack uniformity and consistency. Cybersecurity means different things to different people. All cultures, professions, and individuals in the organization need to understand the cyber-business lexicon.
Critical Thinking Cybersecurity Professionals	There are not enough qualified cybersecurity professionals, and this is not likely to change in the near future. Additionally, cybersecurity and IT are multidiscipline, requiring subspecialists (e.g. system architects, security engineers, software developers, data analysts, network services/administration, computer network defense, forensics…) that often have conflicting capabilities, requirements, and security objectives. Besides appropriately transferring knowledge to grow competencies, good critical thinking and reactionary skills are needed. Cyber analysts must be inquisitive and have good web surfing versus keyboarding skills.
Institutionalizing Effective Behaviors	Positive behaviors are developed through institutionalizing and rehearsing tactics and procedures throughout the organization so that behaviors become habits.
Effective Risk Management	Information risk is business risk. Senior leaders must determine priorities as there are often conflicts at lower levels of management. Organizations are not addressing the most common known vulnerabilities and following basic security procedures. Cybersecurity needs a constant state of motion and agility to adapt; however, this can create a chaotic environment. The ability to proactively protect assets is

Cybersecurity Critical Success Factors	
Critical Success Factor	**Issues and Attributes**
	dependent on how well the system and threat dependencies are modeled and the ability to reconfigure the assets in a timely manner. Changes to network configurations and procedures need tight management which ensures the organization knows what information and systems they possess; the configuration within each system; and, the relationship of that system to others. Selection of system controls should be based on risk and information priorities and data should be secured first, not the networks, applications, etc. Organizations need dedicated risk management resources, skilled in multiple business functions.
Effective Portfolio Management	Managing cyber through a dynamic portfolio process provides an approach to compare, consolidate, and group like security needs in a cost and time effective manner. Non-technical solutions and business process changes are considered first. Cybersecurity considerations must start in the strategy and planning stages and continue throughout lifecycle development, operations, and maintenance. This process includes the supply chain and business continuity. Concept development addresses the performance and security impact on other assets. Cybersecurity professionals must be involved in the investment planning and execution process and collaborate with business functional and financial professionals to determine which solutions meet both the business needs and the cybersecurity and usability requirements, while remaining within budget. Outsourcing and contracts must address the same cybersecurity requirements that the organization follows.
Effective Acquisition and Engineering	Every additional connection, device, or service increases complexity and raises risks. Cyber is built from top-down, from concept development through the entire lifecycle. Requirements are time sensitive requireing that these needs be worked faster in a procurement. Requirements must be tested throughout development and implementation. Poor usability can cause errors that impact security. Careful consideration must be given to an application's ease of use as well as the impact of a cybersecurity requirement on functionality.
Effective Data Segregation	Organizations must move the most sensitive information off networks, partition and encrypt the information that is kept on-line, restrict non-secured and vulnerable websites, and white list sites that employees can access. Tactics, such as honeypots, can be used to collect data on adversaries and divert them from restricted sites.

Cybersecurity and Knowledge Management

A point repeatedly stressed by the focus group is that an organization's success in achieving adequate cybersecurity will not occur if the critical success factors, described above, are not deep-rooted, adequately understood, and embedded and practiced in a timely and agile manner. To address these challenges, the focus group emphasized that training and knowledge management were the primary means to drive change. Change is no easy task. The organization must accurately capture the data and translate it to actionable information and knowledge. It must then, communicate that information to all the various disciplines and cultures within and outside the organization without delay. Organizations need to create a culture of community and belonging so that individuals want to protect information. Individuals and professional groups have many different values, perceptions, and stressors and are motivated by different things. The combination of these factors results in almost infinite outcomes. Co-locating and cross-pollinating people from around the business was found to improve learning and increase the security posture of an organization. Each discipline gained an appreciation for each other's cyber needs and issues.

Cybersecurity Management – A Framework of Interrelationships

A simplified cybersecurity management framework is needed. The focus group stressed the need for a single graphic to convey this. This was the most challenging, and in many respects, the irresolvable aspect of this research. Cybersecurity is more than crosscutting functions. There are many parts in an atmosphere of continual change, interaction, and interdependence among multiple disciplines and functions.

Figure 1 is an overarching cybersecurity management framework. The Critical Enabling Factors are those attributes that an organization must master. No amount of governance, cybersecurity controls or system hardening will prevent cyber incidents without them. First, organizations must show restraint for new , unsecured, technologies and to some extent, information. Second, securing systems requires the integration of all business functions. Every business function is both a "consumer" of cybersecurity and provider to cybersecurity requirements. Business functions need secured information systems. Cyber professionals need to understand the respective business functions' information and systems in order to properly interoperate and secure them. Third, an organization needs the agility and rhythm to monitor, detect, react, respond, and recover from cyber incidents. The data and knowledge management, IT and cybersecurity activities necessary to make this happened are complex and time consuming. Organizations need to be well-rehearsed and skilled in the correct cybersecurity tactics, tools, techniques and procedures to develop this agility and rhythm. Fourth, an organization must achieve a high level of cybersecurity cognition. Developing a skilled and competent cybersecurity workforce is beyond the reach of most organizations. An environment where all employees understand and perform the necessary cybersecurity functions in their day-to-day activities is even harder.

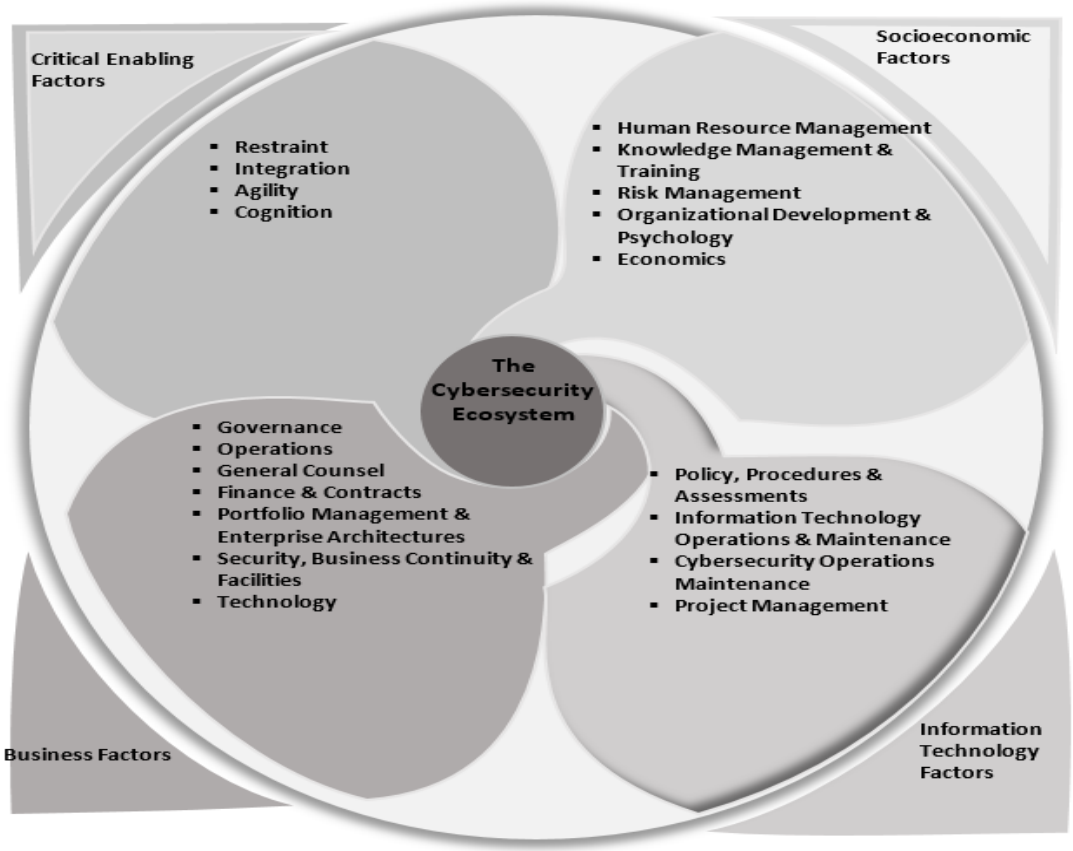

Figure 1. Cybersecurity Management Framework

The Socioeconomic domains represent those areas where human factors and behavior heavily influence outcomes. The Business domains are the standard functions in an organization. The IT subdomains specifically address the policy, procedures, projects and assessments that are germane to cybersecurity to ensure those requirements are integrated into the large corporate governance. It cannot be emphasized enough that these domains are interdependent and in a continual state of change and interaction among multiple stakeholders, disciplines and functions. Understanding this complexity is crucial.

Limitations

There were limitations to this study. The first was time, although the study did reach saturation points in many areas. The data collection period was five months from August to December of 2015. During this time, a content analysis of peer reviewed literature and governance, 19 in-depth interviews, and a focus group was completed. Also, time only permitted for one focus group. Although this was a limitation, the research provided valuable insight into the study of cybersecurity, most notably that agile research approaches and techniques are needed to handle the rapidly changing data, information and technologies that characterize cybersecurity. Finally, while most of the participants had experience in for-profit and non-profit organizations, almost all of them currently support U.S. Government agencies.

RESEARCH

Cybersecurity, Exploratory Research and Meta-Theories

Due to the time constraints of this study, the study was exploratory. An exploratory study implies and indicates that the findings must have further, more in-depth study, examination, and scrutiny. In an "ideal" world, yes. But, is it practical, necessary, and useful for all cybersecurity issues in this early part of the 21st century? This research highlighted three challenges for in-depth research in cybersecurity. These challenges lie in the complex, agile, and interdisciplinary nature of cybersecurity. Research must be thick and quick.

Cybersecurity is interdisciplinary. Multiple groups, with competing interests, have a stake in cybersecurity, both as contributors to the cybersecurity posture of an organization and as a contributor to the factors needed to secure information. Diving into each of these areas, many of which are complex disciplines in themselves, is extremely time consuming. Second, there is a huge amount of cybersecurity data that is quickly needed for decision making but is quickly outdated. Third, many critical success factors continually evolve around interrelationships that are impacted by time, space, events, technologies, and cultures. Although some business, economic, and psychological principles endure over several years, the ability to sufficiently and accurately capture, examine, and vet a comprehensive collective of all findings in an interdisciplinary, holistic field like cybersecurity is practically impossible.

Further, this research was an exercise in agility to know what information was needed for the study, how much was needed, and when to close data collection in order to meet research timelines while at the same time producing current, informative, and actionable material. This study was also a journey that navigated and traversed multiple theories and techniques. Choosing and limiting the number of theories posed a challenge because the management field, particularly with cybersecurity, is impacted by so many factors. An interdisciplinary, meta theory, was a logical choice for this research. In this study a Systems Theory approach was used to develop the cybersecurity management factors and Complexity Leadership Theory, to provide insights into the dynamic, interactive nature between information systems, people, activities and behaviors that must accompany these exchanges. Several other theories could also apply to cybersecurity management, including: Absorptive Capacity, Adaptive Structuration, Cognitive Dissonance, Chaos, Game, Organizational Knowledge, Portfolio, and Fuzzy Logic to name a few.

Cybersecurity and Qualitative Research

Both qualitative and quantitative cyber research methods have value. Quantitative methods, like surveys, can provide a starting point to identify areas and issues requiring further exploration. They can also measure perceptions on effectiveness of policies, procedures, and techniques. The qualitative in-depth interviews, however, developed the detailed cybersecurity ideas and concepts in this study. This study also highlighted the significance of the interrelationship of issues. Interrelationships, or the lack thereof, were identified as the Achilles heel of cybersecurity management. The Focus Group highlighted the importance of these interrelationships in rich detail.

Future Research

This study discussed a broad range of findings, ideas, and thoughts on cybersecurity management. Several of these ideas could benefit from further discussion and research. First is the study of critical success factors. What are they? What are their characteristics? How can an organization address them? The Critical Success Factor section of this paper provides a starting point.

Effective interpersonal relationships are needed to manage cybersecurity. What types, and how much information do the stakeholders need to share? What and how is the best way to share information? Is the cross-pollination of business functions effective? Who should participate, and is the cost of cross-pollinating people reasonable? Is co-locating certain functions effective? What are the most important functional areas to co-locate?

Cybersecurity requires agility. What functions need to be agile? How is agility defined with respect to cybersecurity? What does the agile rhythm look like? How does an organization know when the right rhythm is achieved? How is success measured? When does an organization know when the rhythm is too much or workers are saturated?
Individuals and organizations must be cognitive of cybersecurity issues before they can reflect positive behaviors. A researcher can pursue several questions. What does it mean to be cognitive of cybersecurity? What are the factors? What is information saturation; what does it look like; and, how can managers deal with it?

Cybersecurity is about transferring knowledge and creating the innovation necessary to secure systems. Research is needed to address how cybersecurity learning environments are created and how to tailor the environments for different learning needs and styles. Experimental research methods are one approach. A researcher could utilize experimental research to develop and test learning scenarios along existing frameworks or a newly created framework.

A common lexicon for cybersecurity is needed. Research could examine the challenges of multiple lexicons as well as propose a new one. Case studies could look at government, private sectors, professional organizations, standards, etc. to identify and define those terms. Key research questions examine: What are the cybersecurity terms? In what context are the terms used? What terms should be used; how should they be used; and, when?

The revised NIST RMF was introduced in 2014. Studies should assess its effectiveness. Key questions for the RMF include: Are these the correct components, or is something missing? What are the most important components? What are the most effective components? What information do the stakeholders and players need to perform their duties? What skills and resources are needed by a risk manager?

Resources are limited across organizations and cybersecurity requirements, and solutions are costly and impact every information system. Effective portfolio management of investments is necessary to balance all user and security requirements; select and consolidate the most cost effective approaches; and posture the organization for immediate, emerging, and long-term threats and risks. Research can examine how successful organizations are accomplishing these challenges. How is return on investment and other economic indicators being calculated? It is effective? What are the long-term benefits and challenges with outsourcing? What is the state of the current insurance market? What factors do business and insurance providers need to consider? How effective are risk and loss calculations in accurately estimating the costs of cybersecurity breaches and investments?

Studies are needed to look at cybersecurity acquisition and engineering. How can systems be designed for better usability? How successfull is early lifecycle engagement for cybersecurity? How can agility be brought into acquisitions to adapt to the rapid changes in cyber requirements?

SUMMARY

Cybersecurity is ultimately a leadership and qualitative issue, not a technical problem. Cybersecurity is a business level function, separate from IT and equal to operations, finance, and other primary business functions. Cybersecurity is one of the most, if not the most, interdependent organizational function. The key to improving cybersecurity is the mastery of non-substantive, qualitative, elements. At this time in the 21st century, the world is at a crossroads with information systems and security. Information systems and threats are so complex, multifaceted, changing, and growing that it is nearly impossible, if not completely impossible, to maintain an adequate cybersecurity posture. Even if organizations could afford all the necessary resources, there is a lack of skilled personnel. Another reality for organizations and individuals is their appetite for the newest technologies without regard for security. As long as this appetite persists, security will be an issue. Finally, all organizations, whether industrial, governmental, or academic, should approach an information system issue by first asking, "What is the problem we are trying to solve?" The problem is not technology. Non-technical, innovative, and creative solutions should be a first consideration. By first understanding the underlying problem, the data and information needed to solve the problem will become apparent and will start the process on how best to secure the system.

REFERENCES

Ablon, L., Libicki, M., & Golay, A. (2014). Markets for cybercrime tools and stolen data. Santa Monica: RAND Corporation.

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, *22*(3), 251-264.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Elsevier Information Security Technical Report 17*, 19-25, Available: www.compeseconline.com/publications/prodinf.htm. doi:http://dx.doi.org/ 10.1016/j.istr.2011.12.002.

Control Objectives for Information and Related Technology (COBIT). (2015). Available: http://www.isaca.org/knowledge-center/cobit/pages/overview.aspx

Federal CIO Council. (2012). 2012 Clinger-Cohen core competencies & learning objectives. Retrieved from: https://cio.gov/wp-content/uploads/downloads/2013/02/2012-Learning-Objectives-Final.pdf.

Federal Information Processing Standards Publication. (2006). Minimum security requirements for federal information and information systems. Available: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf U.S. Department of Commerce, National Institute of Standard and Technology. Computer security Division FIPS PUB 200.

Flores, W. & Farnian, A. (2011). Expert opinions on information security governance factors: An exploratory study. In *2011 Proceedings of the ECIS (239)*.

Hughes, J., & Cybenko, G. (2013). Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, *3*(8).

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Security Standard, 27001, (2013). Information security management. Available: http://www.iso.org/iso/iso27001

Jirasek, V. (2012). Practical application of information security models. *Elsevier Information Security Technical Report 17*, 1-8. doi:http://dx.doi.org/10.1016/j.istr.2011.12.004.

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206-2211.

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity; Version 1.0. Washington, D.C. National Institute of Standards and Technology.

Office of Personnel Management, Cybersecurity Resource Center. (2015). Cybersecurity incidents, what happened. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/Learn more about who was impacted and the protections we are working to put into place.

Ponemon Institute Research Report. (2015). 2015 cost of data breach study: global analysis. Ponemon Institute LLC, Michigan, Retrieved on 24 October 2015, available: www.ibm.com/services/costofbreach.

Spradley, J.P. (1979). The ethnographic interview. New York: Holt, Rinehart, and Winston.

U.S. Government Accountability Office. (2015). Federal information system controls audit manual (FISCAM). Available: http://www.gao.gov/financial_audit_manual/overview