Operationalizing Cybersecurity — Framing Efforts to Secure U.S. Information Systems

Dr. Dawn Dunkerley Goss

ABSTRACT

Society has become utterly dependent on information systems (IS) to power everyday life. While this seismic shift has taken place, the security of those IS and their consequential information assets has not taken a front seat alongside innovation, resulting in breaches of trust and loss of corporate goodwill. Organizations are struggling to find an effective approach that encompasses not just technical aspects of cybersecurity, but also improves people and processes. This article will define, discuss, and operationalize the technical, semantic, and effectiveness aspects of cybersecurity and their application into the organizational construct.

INTRODUCTION

IS power an increasing amount of modern infrastructure; from online banking to the social networks connecting disparate friends and family, this reliance on computing systems is unprecedented and can be expected to grow into the future. However, the value of the information itself outpaces the value of the systems storing the information. When calculating the damage created by a breach of cybersecurity, research has shown the greatest damage to be the loss of information resources and their resultant strategic advantages. [1] [2]

Even while organizations are beginning to fully realize the value of their IS and information assets, cybersecurity incidents do occur, and with potentially significant losses. These losses are of both a monetary nature, as well as compromises to information assets. While it can be difficult to determine the full extent of losses suffered through cybersecurity exploits [1] [2] [3], threats certainly have been realized at the corporate, state, and federal levels. The sheer losses borne by organizations fundamentally underline the problems that face corporate entities and nation-states as their infrastructures become increasingly technological and enemies become increasingly sophisticated in their attack techniques.

Dr. Dawn Dunkerley Goss is the Chief of the Cyber Division, Army Materiel Command G-3/4. Her team is responsible for AMC's operationalization of cyberspace to achieve the AMC commander's objectives, facilitate mission command, and maintain AMC's ability to "develop, deliver and sustain" in support of current and future Army and Joint missions.

Dr. Dunkerley received a Ph.D. in Information Systems from Nova Southeastern University in 2011 with a doctoral focus of information security success within organizations. Her research interests include cyberwarfare, cybersecurity, and the success and measurement of organizational cybersecurity initiatives. She holds a number of professional certifications, including the Certified Information Systems Security Professional (CISSP), Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), Information Systems Security Management Professional (ISSMP), Certified Secure Software Lifecycle Professional (CSSLP), and the Certified in Risk and Information Systems Control (CRISC).

Public and private enterprises have developed a number of methodologies to combat threats to their IS and associated information assets. For example, the U.S. Department of Defense has adopted the National Institutes of Standards and Technology (NIST) Risk Management Framework (RMF), a checklist-based approach leading towards an authoritative approval to connect. While these prescriptive, checklist-centric approaches have various sets of controls, they have a common aim: providing a level of security that counterbalances the threats to the IS.

FRAMING AN APPROACH

Many have argued the definition of *information*, perhaps to the unfortunate consequence of this phenomenon containing a bulk of definitions proposed only to serve the narrow interests of those defining them.[6] More recently, literature has placed information into a framework alongside data, knowledge, and wisdom. The data-information-knowledge hierarchy describes data as "a set of signs formulated in a structure and governed by formal rules being processed and interpreted to form information".[7] This information is transformed into knowledge as it is combined with context and personalized into organizational "know-how".[8] Kane (2006) suggested that data, information, and subsequent knowledge are indistinct entities along a single continuum.[9] This is crucial in the context of this research, as the end benefits provided by knowledge synthesis and exploitation are impossible if the information itself is irretrievable, unusable, or without value.

The concept of the *information system* has similarly been debated with varying outcomes. While many see the domain and corresponding terminology in technical terms only[10], IS surpasses a broader swath of understanding than this narrow definition belays. Understanding what encompasses an "infor-

mation system" is fundamental to understanding its role in the organizational context. Does an IS consider both the technology and the personnel using that technology? Does it also consider the organizational constructs enabling both the underlying infrastructure and the personnel through policies and procedures? O'Donovan and Roode (2002) suggested that IS cannot only be concerned with the exploitation of technology but must also consider the effects of technology and the changes—both challenges and opportunities—it can bring. [11]

Many researchers have attempted to define IS on the basis of levels representing these inherent contradictions. Shannon and Weaver (1949) described an IS as having three distinct levels: "technical", defined as incorporating the production of the information; "semantic", defined as the success in conveying the intended message to the receiver; and finally, "effectiveness", described as the level of effect the information actually has on the receiver. [12] Shannon and Weaver clearly believed that the technical must co-exist alongside the socio-organizational aspects to fully encompass the definition of an "Information System". This article will consider the previous passage and adopt the definition presented by Liebenau and Backhouse (1990) defining an information system as an aggregate of information handling activities at the technical, formal and informal levels of an organization. This definition provides an effective representation of the various aspects of consideration within an IS: the technical level includes the information technology present within the organization, the technology is often mistaken as the IS itself. The formal level includes the bureaucracy, rules, and forms concerned with the inter-organizational and the intra-organizational use of information. Finally, the informal level includes the organizational sub-cultures where meanings are established, intentions understood, beliefs, commitments, and responsibilities are made, altered, and discharged. [13]

While organizations are beginning to realize the value of their IS and information assets, cybersecurity incidents do occur, and with potentially significant losses.

Anderson (2003) argued that many definitions of *information systems security* described the processes or concepts adopted towards IS security (hereafter referred to as cybersecurity) without defining the end state—again considering the means without the end. [14] Many definitions of cybersecurity focus on the concepts of Confidentiality, Integrity, and Availability, the so-called CIA Triad, while other research adds attributes such as authenticity and non-repudiation. However, this research is based on the perspective presented by Anderson (2003) that, while these individual notions are worthy goals to be achieved, they are not the "end state" of a cybersecurity program and should not be viewed as such.

Anderson (2003) further argued that a proper definition of cybersecurity must be both flexible and attainable, and support the organizational context in which it is implemented. This passage will adopt the definition of cybersecurity adapted from Anderson (2003) and Dunkerley and Tejay (2012) of "a well- informed sense of assurance that information risks and information security controls are in balance." [15] This definition promotes the concept of balance within an organizational cybersecurity program that considers both the security of the IS and its concomitant data while not tossing the business objectives out the door at their expense. It is key to remember that this definition may differ widely between organizations and sectors (public versus private), based on the sensitivity of the information assets and the nature of the organization itself. For example, healthcare organizations will have a different set of requirements than a military organization and must adjust accordingly.

PAST EFFORTS IN FRAMING

TECHNICAL CYBERSECURITY

Technical research has dominated the field to date. [16] Studies and resultant frameworks have been developed to determine the proper set of technical controls that will secure an organization's IS infrastructure. Some examples of these studies include: encryption, focused on security of the IS's data assets [17] [18]; digital signatures that assure non-repudiation [19] [20]; application security, designed to strengthen the applications hosted by the IS [21] [22] [23]; finally, hardware infrastructure including intrusion detection and firewalls. [24] [25] [26] [27] [28]

When calculating the damage created by a breach of cybersecurity, research has shown the greatest damage to be the loss of information resources.

Technical research has largely focused on protecting infrastructure by facilitating the classic CIA (Confidentiality, Integrity, and Availability) triad, while occasionally interspersing theories developed within the social, criminological, or behavioral domains. CIA has become such a cornerstone of cybersecurity that while a host of other factors have been proposed, such as responsibility, trust [29], non-repudiation and authenticity [30], the CIA triad is the fundamental core of the domain. Most frameworks and policies have been based on the pursuit of these fundamental principles, and many studies assume that achieving the CIA of an organization's assets is the end game of a cybersecurity program. [29] [30] [31] [32] [33] [34] [35] [36]

Anderson (2003) argues, however, that true cybersecurity is not only CIA, and that to fully secure an organization, there must be metrics accompanying the CIA principles.

Further, Anderson urges metric development, not only for CIA but also for the quantification of the value of the cybersecurity program and how the program provides the organization and its stakeholders a "well assured sense of assurance" (p. 313).

ANALYSIS AND MANAGEMENT OF RISK

Risk management is often part of an organizational construct that includes governance and policies [37]. This harkens back to the concept of balance: within a cybersecurity program, the security risks of the organization must be considered alongside the organizational strategies to maximize gain while minimizing loss [38]. However, this strategy assumes that the organizations understand the risks to their organization, which research shows is rare; in fact, it appears that more organizations would be glad to accept risk management theories if they understood the inherent risks to their organization and how to implement a risk management program [39].

Risk management research assumes that a clear analysis and understanding of risks is critical to achieving effective security within an organization; the goal, then, of risk analysis is to help management make informed decisions about investments and to develop those risk management and cybersecurity policies [37]. To properly conduct this process, the organization must then consider the constraints in place inherent to the organization [40]. Risk analysis methodologies measure risk in one of two ways: either as the probability of a negative outcome, or a product of the probability of a negative outcome due to a threat and the probability that the corresponding control will fail to eliminate the threat [41] [42] [43]. To that end, many IS risk analysis methodologies are prevalent across academia and industry. These include quantitative method (e.g., expected value (EV) analysis [41] [42] [43]), stochastic dominance approach [45], Livermore Risk Analysis Methodology (LRAM) [42]), qualitative methods (e.g., scenario analysis, questionnaire, and fuzzy metrics), and tool kits (e.g., Information Risk Analysis Methodologies (IRAM), the CCTA Risk Analysis and Management Method (CRAMM) [40], National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-37, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method [46]. In turn, risk analysis methodologies have evolved from more checklist-based approaches [37] to include more sophisticated theories such as Theory of Belief Function (e.g. [40] and finally, strategic conceptual modeling approaches [47].

> Studies and resultant frameworks have been developed to determine the proper set of technical controls that secure an organization's IS infrastructure.

An effective analysis of risks requires an understanding of what threats are present. A number of studies have attempted to classify threats into various taxonomies, to include categorical [48], results-based [49] [50], empirical data-based [51] [52], matrix-based [53] [54], and process-based [55].

Risk analysis methodologies have been criticized for a variety of perceived weaknesses [56], including over-simplification [57], lack of a scientific approach [58], lack of lucidity [59], and the random nature of actual attacks [60]. Further criticisms have been leveled at functionalist approaches to risk analysis, which claim that organizations over-rely on risk analysis as a predictive model without fully considering other fundamental factors, as the user's behavior [58] [61]. Again, the user is key: research has shown that human risk taking occurs not only through cybersecurity incidents [62] but also through poor decision making when an incident occurs [63]. Again research shows that when the technical aspects are considered without a full understanding of the psychological and cultural variables, the results are not as useful [64]. All things considered, risk analysis is considered valuable by many researchers—even those critical of the current methods—as a process containing merit, if only for providing order to chaos and helping to gain management support for the cybersecurity program [58].

Cybersecurity evolved with a reliance on checklists and other "one-size-fits-all" measures aimed at finding the specific minimum control set that will best protect information systems.

Risk analysis is just one part of the risk management process that has been considered; after threats have been assessed and risks determined, the management of those risks is key—with the ultimate goal maximizing gain for the organization while minimizing loss [38]. This is a long-term process with outputs that feed directly into a healthy governance model, with the expectation that senior management must fully understand organizational risk in order to incorporate it into the strategic outlook. To this end, risk management is not a tool for reflection; risk management, when executed properly, directly contributes to organizational effectiveness [65], should be proactive innature [38] and should be integrated into business processes [66].

Risk management involves a calculated application of selected controls. Straub and Welke (1998) posited that, based on the extant research, controls would fall into one of four distinct categories: deterrence, prevention, detection, and recovery. Studies suggesting controls often use General Deterrence Theory to provide explanations their proposed method will be effective at controlling risk. A number of methodologies have

been developed to facilitate risk management implementation including the Business Process Information Risk Management (BPIRM) approach [35] [66], the Fundamental Information Risk Management (FIRM) methodology [67], and the Perceived Composite Risk (PCR) metric [68].

However, in spite of the research conducted, the methodology followed, and the controls implemented, researchers have argued that there will always be a residual amount of risk to an IS, regardless of the actions taken or decisions made [39] [38] [40] [68]. Risk management, while unable to completely solve the issue of risk, can provide a measure of mitigation.

CYBERSECURITY POLICY, STANDARDS, AND CHECKLISTS

While not as thoroughly studied as purely technical controls [39], it has been argued that one of the most important cybersecurity controls that can be introduced into an organization is the cybersecurity policy [69] [70] [71] [72] [73]. Studies have suggested that most cybersecurity decisions within small to medium-sized organizations are directly guided by cybersecurity policy [74] while large organizations institutionalize cybersecurity in their culture through the use of cybersecurity policy [75]. The term "policy" itself has been argued, with Baskerville and Siponen (2002) dividing research into two schools of thought: technical/computer security and non-technical/management security. Technical security policy generally refers to the automated implementation of management policies [76] [77]. This is confused by the term "policy" being used in technical contexts, such as group policies in a directory environment, or access control policies on a firewall. Management policy, as defined within Baskerville and Siponen (2002), is a high-level plan embracing the organization's general security goals and acceptable procedures. Within this perspective, there has been significant study conducted as to the role of cybersecurity policy within the organization.

One area of cybersecurity policy research has worked to inform the development of effective cybersecurity policies, to include the determination of proper scope and breadth [73] as well as key internal and external influences during development [78]. Baskerville and Siponen (2002) suggested a "meta-policy" or policy for the development of policy, as the best method for developing effective cybersecurity policies tailored to an organizational perspective.

Another area of cybersecurity policy research has focused on the human interaction with cybersecurity policy, from the senior management [70] [79] [80] [81] [36] to the end user [82] [72] [83]. D'Arcy and Hovav (2007) suggested that the human interaction has the potential to completely invalidate the effectiveness of security policies, but also that proper implementation of policies within an organization has the potential to reduce misuse [147].

Finally, it has been argued that for the cybersecurity program to be successful, cybersecurity policy must be aligned closely with the needs of the organization. Researchers

have found that organizations have unique needs that must be considered [71] [84] and that a one-size-fits-all perspective is not ideal; further, inflexibility in cybersecurity policy can encourage "developmental duality" or an imbalance between cybersecurity and usability [85]. Research has shown that policies must be as flexible to the changing needs of the organization, as the changes are fluid, facilitating rather than inhibiting organizational emergence [75].

Another segment of cybersecurity research has focused on the development of standards-based security, such as the Generally Accepted Systems Security Principles (1999) and the ISO/IEC 27000 series. These frameworks purport to best secure anything from an individual asset to an entire organization through implementation of a set of controls, usually covering people, processes, and technology.

Understanding how to create value—investing the optimal amount in protecting assets and creating balance—is key.

Cybersecurity evolved with a reliance on checklists and other "one-size-fits-all" measures aimed at finding the specific minimum control set that will best protect information systems in general [86]. These measures have evolved primarily from the government sector, which has attempted to achieve cybersecurity success through the use of regulated certification and accreditation requirements. The U.S. government, for example, has developed a series of control frameworks (e.g., Department of Defense Information Technology Security Certification and Accreditation Program (DITSCAP), Department of Defense Information Assurance Certification and Accreditation Program (DIACAP), Risk Management Framework (RMF)) that mandate sets of controls across the board based on the integrity, availability, and sensitivity requirements of the IS. These required controls often involve lengthy risk assessments and documentation creation along with stringent technical controls, attempting to secure the people, processes, and technology that power the IS. Internal or third-party certification exercises are often required to validate the implementation. After successful accreditation is received, regular reporting requirements are the norm. Finally, the process is often required on a recurring basis dependent on the sensitivity of the IS.

Closely related to certification and accreditation frameworks are IS governance and management frameworks. While the context [35] [87] [88] differs from governmental control structures, they are very similar in their stated goals: cybersecurity frameworks attempt to ensure the CIA of business information coming into contact with the people, processes, and technology that comprise everyday business operations [89] through the use of mandated controls. Cybersecurity governance and management frameworks have evolved from IT

governance and management frameworks, such as the Control Objective for Information and Related Technology (COBIT) and the Information Technology Infrastructure Library (ITIL). These frameworks have a very limited focus on cybersecurity, with a small number of controls considered alongside other areas like service desks. Purely cybersecurity frameworks, such as the ISO/IEC 27001 (formerly the BS 7799/ISO 17799), have included the Plan/Do/Check/Act cycle that evolved from IT governance frameworks, implementing cycles to establish controls, implement controls, assess controls, and refine based on the results of assessment. These standards have developed within industry, but academia has begun development of frameworks that attempt to apply cutting-edge theories for industry practice. An example is the von Solms and von Solms (2006) Direct-Control Model, and the Business Model for Information Security, developed through the University of Southern California (ISACA, 2009) and licensed through the Information Systems Audit and Control Association.

Finally, cybersecurity maturity criteria have been a burgeoning topic of research. Maturity criteria aim to offer an objective scale for classifying an organization's cybersecurity posture, from low to high. These criteria not only offer a "goal" for improvement but also can be viewed as differentiating an organization from its competitors based on a quantified assessment of successful cybersecurity control implementation. The System Security Engineering Capability Maturity Model, a product of research done at Carnegie Mellon University has received the most attention [90], but alternate models do exist.

ECONOMICS OF CYBERSECURITY

As information as an asset increases in importance, many researchers [93] [94] [95] have discussed the organizational value of information systems and how their protection supports and furthers the business as a whole. Since most measures—technical, personnel, procedural—involve some level of resource allocation, spending on cybersecurity has become an important priority within organizations [94]. Understanding how to create value—investing the optimal amount in protecting assets and creating balance—is key. A good deal of research has focused on deriving the optimal amount for an organization to invest in securing their IS and related assets [96] [97] [98] [99] [100] [101] [102] [93] [103] [94] [95]. This research stream has culminated in the development of models for predicting this optimal amount of cybersecurity investment e.g., [94] [104] [105]. Finally, as large amounts of money are allotted for cybersecurity measures, stakeholders have begun to demand results that they can see, to justify these expenditures. Traditional economic ideas, such as Return on Investment (ROI), have been discussed, with researchers attempting to determine if tools such as Return on Security Investment (RoSI) [94] and the Analytic Hierarchy Process (AHP) [105] would be useful for explaining cybersecurity investments.

A further factor that has been considered is the true cost of IS insecurity; it has been found that there is a highly significant negative market reaction to cybersecurity breaches,

especially when involving unauthorized access to confidential data [107]. This fact is further compounded for certain market segments, such as Internet-specific firms and software vendors, who are subjected to even greater risk of losses due to security breaches [108] [109]. Further, research has shown that even unpublished breaches can have a devastating economic effect on a firm [111]; organizations cannot hide from their vulnerabilities and expect to come out unscathed. Incentives are not only monetary, however; multiple studies have discussed the incentives created by regulations like the Sarbanes-Oxley Act [111] [104]. Within these guidelines, there are often economic penalties for non-compliance. This is another economic factor that must be considered when quantifying the cost of cybersecurity.

It is important for stakeholders to stress the value that cybersecurity can create within an organization; however, when attempting to explain how a cybersecurity program creates value for an organization, one cannot focus solely on economic aspects. Research has discussed at length the socio-organizational considerations involved with cybersecurity, such as effects on organizational culture, and their value to the organization [112] [113] [114] [115].

To shed new light on internal threats using fresh perspectives criminological theories have been introduced to the IS domain.

THE USER

Research has suggested that cybersecurity has an almost "self-canceling" phenomenon to consider: the user [116]. Lack of user compliance has been directly tied to a decrease in cybersecurity effectiveness [77]. Since the effectiveness of controls that are put in place to protect information assets are constrained by behaviors of human agents who access, use, administer, and maintain them [30][118] [119], it is clear that the user and their effect on cybersecurity must be considered. Anderson (2001) even argued that information insecurity is as much due to "perverse incentives" as it is to weaknesses in the technical infrastructure.

One line of research deals with counterproductive computer usage and malicious extremes, including insider threats [121] [122] [123] [124] [125] [126] [119] [127] [128]. While firms are shown to spend more resources countering perceived threats originating from external forces [119], it has been argued that the insider threat is perhaps the most significant threat an organization should consider [121] [126] and that the actual number of internally-led breaches suffered cannot be known due to the vast amount of unreported and unknown breaches [127]. Much research centers around General Deterrence Theory-based approaches to solving insider threat [129] [130], theorizing that misuse will decrease as the disincentives increase. Further, studies have shown that increasing internal knowledge of cybersecurity policy and other countermeasures, while not consistent, has the effect

of decreasing misuse from certain internal groups [127]. However, policy alone cannot be relied upon as a deterrent; Siponen, Pahnila, and Mahmood (2010) found social pressures, employee assessments of vulnerability, and the immediacy of threats all play a part in determining employee intention to comply with cybersecurity policy. To shed new light on internal threats using fresh perspectives, criminological theories have been introduced to the IS domain [131].

Another group of research focuses on external threats. These are the threats perhaps most closely identified as hacking [104] or competition [132]. Stanton et al. (2005) found that firms are more concerned with threats originating from external sources; this is perhaps due to the dominance of externally exploited breaches reported in the press [107]. Studies have shown that the perception of external threats—hackers, viruses, and spyware—so dominate cybersecurity programs that even security policy development first considers protection against the external, rather than internal, threat [133]. Research has typically considered the external threat to be fixed and immutable [134], but it has been suggested that external threats do consider the costs and benefits of attack based on information identified through competitor analysis [132].

Another major theme emerging within the cybersecurity domain is the importance of considering the human factor.

A second subset of user research focuses on the awareness of users towards the systems—both the information system and its protective technologies—with which they interact [123] [145]. Research has shown that awareness of technology is central to the formation of user attitudes, and in turn, the user's concern for cybersecurity [136] [137] but is difficult to characterize due to the individual nature of the variable itself [116]. For instance, awareness towards the negative consequences of spyware has been found to motivate users to develop positive attitudes towards protective technologies and their intention to use them [115]. However, research suggests that simply telling users to follow secure practices is not enough; they must be convinced of it [138].

Another research stream attempts to better understand the user's intentions and their effect on cybersecurity. These studies often incorporate theories such as the Theory of Planned Behavior or Theory of Reasoned Action to explain user intention and its effect on subsequent behavior. Research suggests that user intention is affected by a number of external moderators, including organizational commitment [83], codes of ethics [139], cultural factors [140] [115], and social pressures [142]. Further studies have discussed the link between the user's awareness and their intentions towards IS [119] [141] and suggest that user awareness has a direct link to their intentions, which in turn affects behavior. These findings suggest that user intention—ranging from the malicious to the beneficial—might be a key to understanding why users behave in the manner that they do, and the measures that must be taken to prevent or protect against malicious behavior.

MAJOR THEMES OF RESEARCH

The streams of research within cybersecurity differ in their nature, but there are definite themes recurring throughout the domain. Early works within cybersecurity research were significantly technical, and highly prescriptive, with a heavy dependence on checklists and methodological-based approaches aimed at producing a "one-size-fits-all" method of protection. This mindset, while long deemed inadequate by researchers [75] does continue to persist through some governance and standards-based measures currently in use. However, the field as a whole is evolving with the times; researchers have begun to expand into organizational optimization, considering the concepts of balance and emergence. These concepts weave through a considerable number of studies across the cybersecurity domain. An example is the economic research of Gordon and Loeb (2002, 2006), promoting the idea of a balanced cybersecurity program as value maximization by optimal investment into the protection of assets, a highly context-dependent concept. These concepts align with Anderson's (2003) definition of cybersecurity as risks and controls being in balance.

Another major theme emerging within the cybersecurity domain is the importance of considering the human factor present within the IS. While the IS is not solely technical in nature, early research streams within the cybersecurity domain focused primarily on achieving CIA and its fellow tenets through technical methods. A paradigm shift in the domain occurred when the human aspect began to be considered. Da Veiga and Eloff (2007) described cybersecurity as having distinct phases of evolution: the first phase, purely technical in nature, heavily depended on the technological means of securing the IS. The second phase began when the realization was made that the human element urgently needed to be addressed. This realization has been reflected within the body of research; the cybersecurity domain has moved from purely technical considerations to the inclusion of a great number of studies focusing on socio-organizational areas such as culture [140] [115], user awareness [123] [145], and user behavior [119] [141] [142]. Clearly, as research has suggested a powerful mitigating effect presented by the human factor [117] [116], it can be expected that the human factor will continue to be an important consideration across the cybersecurity domain.

Table 1 presents an analysis of cybersecurity constructs regarding Shannon and Weaver's (1949) levels of communication, adapted from Dunkerley and Tejay, 2009 and 2011 [143] [144]. Understanding these factors presented within the structure provided by Shannon and Weaver (1949), the benefits provided through the dynamic relationship between the Technical Level factors (Information Integrity, Information Systems Assurance, and Operations Enablement) and the Semantic Level factors (User Intention and User Knowledge) lead to the Effectiveness Level proffered upon the organization, Cybersecurity Success as adapted from Dunkerley and Tejay (2012) [146].

Communication Levels	Definition	Cybersecurity Dimensions	Seminal Literature
Technical	The accuracy and efficiency of the system producing information.	Information Integrity, Information Systems Assurance, Operations Enablement	Anderson (1972), Wiseman (1986), Denning (1987), Muralidhar et al. (1995), Sandhu et al. (1996), Daniels & Spafford (1999).
Semantic	The success the information has in conveying the intended meaning from sender to receiver.	User Intention, User Knowledge	Dhillon (2001), Siponen (2001), Trompeters & Eloff (2001), Schultz (2002), Vroom & von Solms (2004), Stanton et al. (2005), Dinev et al. (2008).
Effectiveness	Effect of information on the user's behavior.	Cybersecurity Success	Anderson (2001), Gordon and Loeb (2002), Campbell et al. (2003), Hovav and D'Arcy (2003), Tanaka et al. (2005), Arora et al. (2006).

Table 1. Cybersecurity Dimensions for Shannon and Weaver (1949) Communication Levels

CONCLUSION

In an examination of the different aspects of cybersecurity literature, several points are notable. First, an emphasis has been placed on "a means to an end." Research studies have largely focused on measures to address one or more of the technical aspects of cybersecurity, such as an individual aspect of the CIA triad. While this research contributes to the greater understanding of what constitutes that quality of cybersecurity, it is a mistake to believe that only focusing on the technical assets of an organization while failing to consider other dimensions will facilitate a secure organization. Cybersecurity must be viewed as a holistic process rather than a single "fix."

Another issue is with the overwhelming emphasis on individual dimensions as shown within Table 1, without understanding the interactions of those dimensions. A proposed model of cybersecurity success should show a causal process with an intervening factor presented by the user. It is clear that more study should be focused on the entire life cycle of cybersecurity and the interaction between the individual dimensions.

NOTES

1. Center for Strategic and International Studies (CSIS). (2009). *Significant cyber events since 2006.* Retrieved 22 December 2009 from http://csis.org/files/publication/091109_cyber_events_since_2006.pdf.

2. Pisello, T. (2004, October). Is there a business case for IT security? *Security Management.* Retrieved October 18, 2010 from http://www.securitymanagement.com/article/there-business-case-it-security.

3. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

4. Center for Strategic and International Studies (CSIS). (2008). *Securing cyberspace for the 44th presidency.* Retrieved 22 December 2009 from http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf.

5. Gaudin, S. (2007, April 11). Security breaches cost $90 to $305 per lost record. Information Week. Retrieved October 18, 2010 from http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222.

6. Liebenau, J., & Backhouse, J. (1990). *Understanding Information: An Introduction.* London: Macmillan.

7. Tejay, G., Dhillon, G., & Chin, A.G. (2005). Data quality dimensions for information systems security: A theoretical exposition. In P. Dowland, S. Furnell, B. Thuraisingham, & X. S. Wang (Eds.), *Security Management, Integrity, and Internal Control in Information Systems* (pp. 21-39). New York: Springer.

8. Alavi, M., & Leidner, D.E. (2001). Knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly, 25*(1), 107-136.

9. Kane, G.C. (2006). Casting the net: A multimodal network perspective on knowledge sharing. *Dissertation Abstracts International, 67*(09), (UMI No: 1232407861).

10. Lovata, L.M. (1987). Behavioral theories relating to the design of information systems. *MIS Quarterly, 11*(2), 147-149.

11. O'Donovan, B., & Roode, D. (2002). A framework for understanding the emerging discipline of information systems. *Information Technology & People, 15*(1), 26-41.

12. Shannon, C.E., & Weaver, W. (1949). *The Mathematical Theory of Communication.* Urbana, IL: University of Illinois Press.

13. Dhillon, G., & Backhouse, J. (1994). Responsibility analysis: A basis for understanding complex managerial situations. In *Proceedings of the International System Dynamics Conference,* 70-79.

14. Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308.

15. Dunkerley, K., Tejay, G. (2012). The development of a model for information systems security success. In Measuring Organizational Information Systems Success: New Technologies and Practices, IGI Global.

16. Chang, S.E., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

17. Kaliski, B. (1993). A survey of encryption standards. *IEEE Microcomputers, 13,* 74-81.

18. Blythe, S.E. (2008). Croatia's computer laws: Promotion of growth in e-commerce via greater cyber-security. *European Journal of Law and Economics, 26,* 75-103.

19. Rivest, R. L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

20. Tompkins, T., & Handley, D. (2003). Giving e-mail back to the users: Using digital signatures to solve the spam problem, *FirstMonday, 8*(9).

21. Walsh, M.E. (1981). Software security. *Journal of Systems Management, 32*(10), 6-14.

22. Shimeall, T.J., & McDermott, J.J. (1999). Software security in an internet world: An executive summary. *IEEE Software, 16*(4), 58-62.

23. August, T., & Tunca, T.I. (2006). Network software security and user incentives. *Management Science, 52*(11) 1703-1721.

24. Denning, D. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering. 13*(2), 222–226.

25. Daniels, T. E., & Spafford, E. H. (1999). Identification of host audit data to detect attacks on low-level IP. *Journal of Computing Security, 7*(1), 3–35.

26. Vigna, G., & Kemmeerer, R. A. (1999). NetSTAT: A network-based intrusion detection system. *Journal of Computing Security, 7*(1), 37–71.

27. Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information Systems Security, 3*(3), 186–205.

28. Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information Systems Security, 3*(1), 1–29.

29. Krauss, M., & Tipton, H. (2002). *Handbook of Information Security Management.* Boca Raton, FL: CRC Press.

30. Ma, Q., Johnston, A.C., & Pearson, J.M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

31. Hayam, A., & Oz, E. (1993). Integrating data security into the systems development life. *Journal of Systems Management, 44*(8), 16-21.

32. Leiwo, J., Gamage, C., & Zheng, Y. (1999). Organizational modeling for efficient specification of information security requirements. In *Proceedings of the Advances in Databases and Information Systems: 3rd East European Conference (ABDIS),* 247-260.

33. Byrnes, F., & Proctor, P. (2002). *The Secured Enterprise: Protecting Your Information Assets.* Upper Saddle River, NJ: Prentice Hall.

34. Rosenthal, D. (2002). Intrusion detection technology: Leveraging the organization's security posture. *Information Systems Management, 19*(1), 35-44.

35. Moulton, R., & Coles, R.S. (2003). Applying information security governance. *Computers & Security, 22*(7), 580-584.

36. von Solms, S.H. (2005). Information security governance–Compliance management vs operational management. *Computers & Security, 24,* 443-447.

37. McFadzean, E., Ezingeard, J., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. *Journal of Information System Security, 2*(3), 3-48.

38. Kotulic, A.G., & Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management, 41,* 597-607.

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

40. Sun, L., Srivastava, R.P., & Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems, 22*(4), 109-142.

41. Perschke, G.A., Karabin, S.J., & Brock, T.L. (1986). Four steps to information security. *Journal of Accountancy, 161*(4), 104-113.

42. Guarro, S.B. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers and Security, 6*(6), 493-504.

43. Pickard, R. (1989). Computer crime. *Information Center, 5*(9), 18-27.

44. Rainer, R.K., Snyder, C.A., & Carr, H.H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129-147.

45. Post. G.V., & Diltz. J.D. (1986). A stochastic dominance approach to risk analysis of computer systems. *MIS Quarterly, 10*(4), 363-375.

46. Woody, C. (2006). *Applying OCTAVE: Practitioners report.* Carnegie Mellon University.

47. Misra, S.C., Kumar, V., & Kumar, U. (2007). A strategic modeling technique for information security risk assessment. *Information Management & Computer Security, 15*(1), 64-77.

48. Cheswick, W.R., & Bellovin, S.M. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Reading, MA: Addison-Wesley Publishing Company.

49. Russell, D., & Gangemi, G.T. (1991). *Computer Security Basics.* Sebastopol, CA: O'Reilly.

50. Cohen, F.B. (1995). *Protection and Security on the Information Superhighway.* New York: John Wiley.

51. Neumann, P., & Parker, D. (1989). A summary of computer misuse techniques. In *Proceedings of the 12th National Computer Security Conference.*

52. Amoroso, E.G. (1994). Fundamentals of Computer Security Technology. Saddle River, NJ: Prentice-Hall PTR.

53. Perry, T., & Wallich, P. (1984). Can computer crime be stopped? *IEEE Spectrum, 21*(5).

54. Landwehr, C.E., Bull, A.R., McDermott, J.P., & Choi, W.S. (1994). A taxonomy of computer security flaws. *ACM Computing Surveys, 26*(3), 211-254.

55. Stallings, W. (1995). *Network and Internetwork Security Principles and Practice.* Englewood Cliffs, NJ: Prentice Hall.

56. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

57. Kokolakis, S. A., Demopoulos, A. J. & Kiountouzis, E. A. (2000). The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security, 8*(3), 107-116.

58. Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.

59. Alter, S., & Sherer, S.(2004). A general, but readily adaptable model of information system risk. *Communications of the AIS, 14*(1), 1-28.

60. Clements, D. P. (1977). Fuzzy Ratings for Computer Security Evaluation. PhD Dissertation, University of California, Berkeley.

61. Beck, U. (1992). *Risk Society.* London: Sage.

62. Hitchings, J. (1996). A Practical Solution to the Complex Human Issues of Information Security Design. In I*nformation Systems Security: Facing the Information Society of the 21st Century.* London: Chapman & Hall.

63. McGaughey, R.E., Snyder, C.A., & Carr, H.H. (1994). Implementing information technology for competitive advantage: Risk management issues. *Information & Management, 26*(5), 273–280.

64. Webler, T., Rakel, H., & Ross, R. J. S. (1992). A Critical Theoretical Look at Technical Risk Analysis. *Industrial Crisis Quarterly, 6,* 23-38.

65. Jarvenpaa, S.L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly, 15*(2), 205–227.

66. Coles, R.S., & Moulton R. (2003). Operationalizing IT risk management. *Computers and Security, 22*(6), 487-493.

67. Rycroft, S., & Tully, M. (2007). Building an information security meta standard. *BT Technology Journal, 25*(1), 37-40.

68. Bodin, L.D., Gordon, L.A., & Loeb, M.P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64-68.

69. Parker, D.B. (1998). *Fighting Computer Crime– A New Framework for Protecting Information.* New York: John Wiley & Sons.

70. Perry, W.E. (1985), *Management Strategies for Computer Security.* Boston, MA: Butterworth-Heinemann.

71. Schweitzer, J.A. (1982). *Managing Information Security: A Program for the Electronic Information Age.* Boston, MA: Butterworth-Heinemann.

72. Warman, A.R. (1992), Organizational computer security policy: The reality. *European Journal of Information Systems, 1*(5), 305-310.

73. Hone, K., & Eloff, J.H.P. (2002). Information security policy–What do international information security standards say? *Computers & Security, 21*(5), 402-409.

74. Briney, A., & Prince, F. (2002). Does size matter? Accessed from www.infosecuritymag.com/2002/sep/2002survey.pdf.

75. Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

76. Sterne, D.F. (1991). On the buzzword 'security policy'. *In Proceedings of the IEEE Computer.*

77. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

78. Tanenbaum, A. (1992). *Modern Operating Systems.* Englewood Cliffs, NJ: Prentice-Hall.

79. 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.

80. Gondek, C. (1989). Establishing information security. *Management Accounting, 70*(10), 34-37.

81. Kwok, L., & Longley, D. (1997), Code of practice: A standard for information security management. In *Proceedings of the IFIP TC11 13th International Conference on Information Security.*

82. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

83. Belden, M. (1989). The employee's role in protecting information assets. *Computers & Security, 8*(6), 487-493.

84. Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-126.

85. Wood, C.C. (1999). *Information Security Policies Made Easy.* San Rafael, CA: Baseline Software.

86. Baskerville, R. (1992). The developmental duality of information systems security. *Journal of Management Systems, 4*(1), 1-12.

87. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375-413.

88. Poore, R. (2006). Information Security Governance. In Handbook of *Information Security Management.* Boca Raton, FL: CRC Press.

89. Da Veiga, A., & Eloff, J.H.P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

90. Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23,* 638-646.

91. Siponen, M.T. (2005). Analysis of modern IS security development approaches: Toward the next generation of social and adaptable ISS methods. Information and Organization, 15, 339-375.

94. Anderson, R. (2001). Why Information Security is Hard—An Economic Perspective. In Proceedings of 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, 10-14.

95. Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

96. Gordon, L.A., & Loeb, M.P. (2006). Budgeting process for information security expenditures. Association for Computing Machinery. *Communications of the ACM, 49*(1), 121-125.

97. Millen, J. (1992). A resource allocation model for denial of service. In *Proceedings of the 1992 IEEE Symposium on Security and Privacy.* Los Alamitos, CA: IEEE Computer Society Press.

98. Luotonen, O. (1993). *Risk management and insurances.* Painatuskeskus Oy, Helsinki, Finland.

99. McKnight, L., Solomon, R., Reagle, J., Carver, D., Johnson, C., Gerovac, B., Gingold, D. (1997). Information Security of Internet Commerce. In *Internet Economics.* Cambridge, MA: MIT Press.

100. Finne, T. (1998). A conceptual framework for information security management. *Computers & Security, 17*(4), 303–307.

101. Jones, M.R. (1997). It all depends what you mean by discipline. In Mingers, J., & Stowell, F. (Eds.), *IS: An Emerging Discipline?* London: McGraw-Hill.

102. Buzzard, K. (1999). Computer security-What should you spend your money on. *Computers & Security, 18*(4), 322–334.

103. Hoo, K. (2000). How much is enough? A risk-management approach to computer security. A Consortium for Research on Information Security Policy (CRISP) Working Paper. Stanford, CA: Stanford University.

104. Meadows, C. (2001). A cost-based framework for analysis of denial of service in networks. *Journal of Computer Security, 9*(1/2), 143–164.

105. Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25,* 629-665.

106. Huang, C.D., Hu, Q., & Behara, R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114(2) 793-804.

107. Bodin, L., Gordon, L.A., & Loeb, M.P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78-83.

108. Campbell, K., Gordon, L.A., Loeb, M.P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security,* 431-448.

109. Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

110. Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering, 33*(8), 544.

111. Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers, 8*(5), 350-362.

112. Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Sohail, T. (2006). The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. *Journal of Accounting and Public Policy, 25*(5), 503-530.

113. Backhouse, J., Hsu, C.W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly, 30,* 413-438.

114. Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16,* 293-314.

115. Drevin, L., Kruger, H.A., & Stegn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26,* 36-43.

116. Dinev, T., Goo, J., Hu, Q., & Nam, K. (2008). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

117. Dodge, R.C., Carver, C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security, 26,* 73-80.

118. Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

119. Stanton, J.M., Stam, K.R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 24,* 124-133.

121. Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171–175.

122. Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20,* 165-172.

123. Siponen, M.T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal, 14*(4), 15-23.

124. Trompeters, C.M., & Eloff, J.H.P. (2001). A framework for the implementation of socio-ethical controls in information security. *Computers & Security, 20,* 384-91.

125. Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531.

126. Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91–95.

127. D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89,* 59-71.

128. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105.

129. Tittle, C. R. (1980). *Sanctions and Social Deviance: The Question of Deterrence.* NY: Praeger.

130. Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

131. Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems, 15,* 403-414.

132. Gordon, L.A., & Loeb, M.P. (2001). Using information security as a response to competitor analysis systems. Communications of the ACM, 44(9), 70-75.

133. Smith, H.J. (1994), *Managing Privacy: Information Technology and Corporate America.* Chapel Hill, NC: University of North Carolina Press.

134. Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26,* 639-688.

136. Goodhue, D.L., & Straub, D.W. (1991). Security concerns of system users: A study of perception of the adequacy of security measures. *Information and Management, 20*(1), 13–27.

137. Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

138. Pfleeger, C.P., & Pfleeger, S.L. (2003). *Security in computing* (3rd ed.). Prentice Hall.

139. Harrington, S.J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

140. von Solms, B. (2000). Information security – The third wave? *Computers & Security, 19*(7), 615-620.

141. Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

142. Siponen, M., Pahnila, S., & Mahmood, M.A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

143. Dunkerley, K., Tejay, G. (2009). Developing an information systems security success model for e-government context. In Proceedings of the 2009 Americas Conference on Information Systems, San Francisco, CA.

144. Dunkerley, K., Tejay, G. (2011). A confirmatory analysis of information systems security success factors. Hawaii International Conference on System Sciences.

145. Thomson, M.E., von Solms. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167.

146. Dunkerley, K., Tejay, G. (2012). The development of a model for information systems security success. In Measuring Organizational Information Systems Success: New Technologies and Practices, IGI Global.

147. D'Arcy, J., & Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information Systems Security, 3*(2), 3-30.