The Utility of Security Standards

Jennifer L. Bayuk, *Member, IEEE*

***Abstract*—This paper describes a method for analyzing systems security using a soft systems engineering approach. It uses a systems engineering modeling tool to demonstrate systemic attributes of security that are common across systems. It describes how the approach is being used to model security standards.**

***Index Terms*— computer security, cybersecurity, systems security, systems engineering**

I. Introduction

Information systems security control practices are published in the form of *standards* by organizations whose members are widely respected for cybersecurity expertise. [1-10] are examples. These standards have been adopted and endorsed by both public and private sector information security assessment teams. Systematic application of these standards has become synonymous with management due diligence in establishing control over electronic systems. By incorporating these standards into their own security assessment processes, many audit and regulatory organizations have tacitly characterized information systems security as a state of compliance with these standards.

The vast majority of these standards have been established by committees of stakeholders in security outcomes. Communities of auditors have played major roles in establishing these standards. Major banks and financial institutions have made major contributions to these standards. Government agencies have been chartered with drafting standards, sending them out for comment to scores of volunteer contributors, and incorporating contributor comments into the final result. Specific recommendations included in these standards are repeated in multiple instances of them. There is no doubt that the vast majority of information security professionals agree that such standards provide sound advice for achieving security goals. Nevertheless, there has not been formal scientific study on the effectiveness of these standards in accomplishing organizational security objectives.

This paper describes a way to evaluate the utility of generally accepted cybersecurity standards. It is not intended to be an endorsement of any standard, or of standards in general. Rather it describes a systems engineering approach to the investigation of security standards utility in identifying security requirements and modeling systems security.

Manuscript received July 30, 2010. This work was supported by the U.S. Department of Defense and the NSA under contracts H98230-08-D-0171 and FA8240-07-C-0141-P00004.

Jennifer Bayuk is with Stevens Institute of Technology, Hoboken, NJ 07030 USA (973-335-3530; fax: 973-335-0789; e-mail: jennifer.bayuk@stevens.edu).

II. Systems Engineering Concerns

The systems engineering community is concerned with the ability of current security standards to accomplish expectations for systems security [11]. Historically, cybersecurity standards have been applied to information processing systems in isolation, or electronic components of systems. They are not easily adapted to systems with mechanical or operational security features. Some, like ISO 27001 [7], describe security management, and so may applied to an entire enterprise or organization taken as a system. However, at the security risk assessment level that produces customized systems security requirements, this is not often done in practice [12].

An organization often recognizes the criticality of security to a given computer application, and will establish controls over that one system but not the whole enterprise. Security requirements have also been motivated by stakeholders external to an organization; for example, by a customer's requirements for information protection or by a regulator's requirement for information confidentiality. Scope criteria for the application of security standards has therefore typically been limited to the objectives of a given security audit or assessment. Such fragmentary approaches have been extended to security assessment in general, even at the requirements stage of the system lifecycle. Systems engineering curriculum identifies security requirements as optional capability rather than a core function [13].

Even where an enterprise-wide view is encouraged, standards for organizational security allow for sets of devices identified in a given inventory to define the scope of a systems security assessment (e.g. [14]). This guidance prompts an organization to execute security measures only for devices that they directly control. Systems interfaces are sometimes covered only to the extent that an organization is obligated by a stakeholder to assess a business partner's ability to protect information of particular interest. Yet, even those third party assessment standards specifically designed to test the extent to which business partners are secure do not address nonstandard interfaces between enterprises (e.g. [3]).

In general, security standards tend focus on reducible system components rather than complex system processes like information flow. They focus on checklists with respect to organizational assets supported by the system and do not take into account the systemic security attributes of the system itself. For example, where standards provide guidance on how to classify information, it is in terms of impact to the organization of harm to the information's confidentiality, integrity, and availability. Such approaches are rooted in the

978-1-4244-7400-4/10/$26.00 ©2010 IEEE

military's three-tiered classification of top secret, secret, and unclassified information. They do not transfer to today's complex systems environments [15].

In most of these standards, systems owners and operators are advised to ensure that there are decision-makers qualified to conduct security risk assessments. These individuals are expected to be omniscient with respect to the information content of their enterprise and are expected to be able to quantify the impact of harm to that content. That content is expected to be amenable to a catalogue-like process that will allow systematic application of a suite of technology control measures. The guidance is too generic to cover systems characteristics that are unique to a given enterprise. For example, in a complex job processing system that transfers files from a common repository to business partners, a security assessment based on today's standards would classify the information, and based on its value, identify and closely inspect technical controls. But it would not specify the approval and oversight process designed to ensure that each business partners receive only their own data beyond a generic "need to know" confidentiality requirement. These requirements would be left to the judgment of a data owner or custodian. In practice, they would typically be left to business logic within software applications. Even if the scope for a security risk assessment was complete and accurate, all standards include guidance that systems owner and/or custodians should be the judge as to whether a recommended control is necessary in every case.

Figure 1 is an example excerpt from a typical security standard [10]. It advises that systems must be inventoried and the degree to which each inventory item supports the enterprise should be assessed in a few dimensions that map to generic security requirements. Its next advice is to give the inventory item itself some kind of rating that can be used to derive a security requirement, which is a recommendation for a technical control measure.

Figure 1: Example of a Security Standard

Special Publication 800-53, Revision 2 — Recommended Security Controls for Federal Information Systems

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
	Access Control			
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7

Where these methodologies provide guidance on how to make decisions on technical security controls, security managers are encouraged to make technical implementation decisions by systematically listing threats, placing probabilities on the likelihood of those threats, and then comparing the cost of a known remediation activity to the cost of damage that would occur if the threat was enacted. This low level guidance shares flaws inherent to the rating methodology in that both rely on subjective assessments of probabilities in an incomplete problem space.

Figure 2 is a generic diagram of a security standard. The diagram simplifies but does not exaggerate the structure of today's security standards. Today's standards contain little guidance by way of methods, processes, or tools with which to analyze systems or system components and create relevant security requirements. Nor do they provide guidance on how to question a system owner or operator as to the judgment on whether a control is necessary. Hence, they are reducible to instructions in technical implementation, which, as noted above, are generally agreed to be sound.

Figure 2: Diagram of a Security Standard

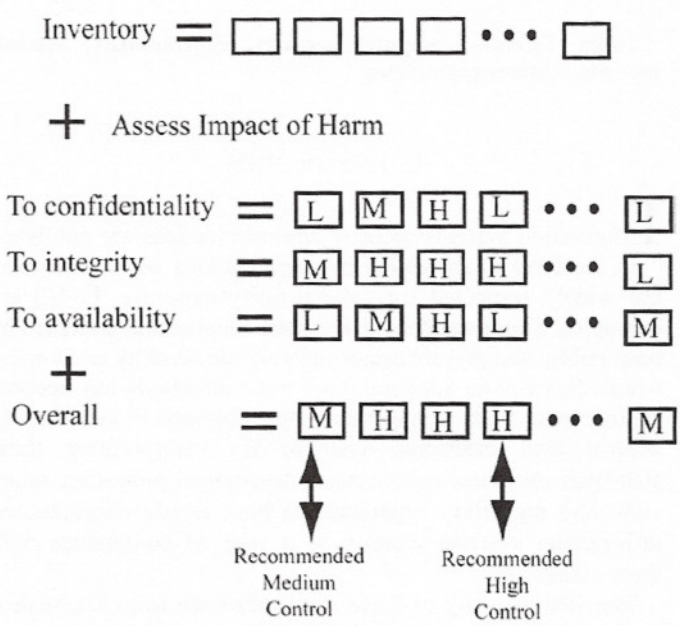


Figure 2 is meant to illustrate that the bulk of the true analysis work in a traditional security risk assessment is in the method by which a system is catalogued and divided in ways that its component's impact on mission can be assessed, and that today's standards lack guidance in that critical step of the process. The result is that security assessment methodology is a relatively straightforward technical implementation recommendation for low level controls. It is incomplete, and it does not contribute to a holistic understanding of the security properties of the system. As it does not begin to analyze the root causes of security issues, which stem from security attributes of the system infrastructure itself, such methodology is bound to fail, and it is not surprising that such failure corresponds to the state of security engineering in general.

III. Security Defined

Consistent application of cybersecurity standards using expert security risk judgment have been refined and adopted over the years, and probably does increase the overall

cybersecurity level of the system itself by the technical measure. The word "probably" is used to modify the previous statement because there have actually been no studies that prove whether or not such diligence in security configuration does increase security. This situation calls attention to the fact that there is no consensus on what it means to be secure. Evidence does exist that security may reduce productivity and adversely impacts system function and thus reduces value [16].

Anecdotal research has correlated management practices with good security as defined by "best in class" organizations [17, 18]. These studies have identified the control practices that each "best in class" organization uses to maintain security, and concluded that the intersection of those practices should be adopted by others. As a research method, this approach is weak because it projects conclusions that are internally valid in small samples onto a much larger unobserved population [19]. It also begs the question on what it means to be secure. A holistic systems approach would include a wider variety of organizations and systems in the scope for a review, and identify more attributes in a construct theory of security.

Where problems are not well-understood but the need for solutions persists, the systems engineering tool of choice will be a soft systems methodology (SSM) [20]. SSM methodology involves iterative modeling exercises that employ feedback loops to evaluate a model's utility in system representation. In our application to security, we want to know whether applying a security standard results in system operation to corresponding practical and obvious organizational goals for security [21, 22]. A gap analysis on results may be performed, and security standards may be evaluated according to their utility in achieving organizational security objectives. Such an exercise may also facilitate the identification of key controls within standards, if any, that appear to have greater utility than others.

In any such study of security standards, the first step must be to clarify what is meant by security. We must also clarify the security recommendations included in a given security standard. To this end, we adopt a soft systems engineering tool called a systemigram [23]. The word systemigram was coined by as a convergence of "system" and "diagram." It was envisioned as a tool to assist systems engineers in covering a topic without sacrificing detail required to accomplish clarity. A systemigram starts with the system to be defined at the top left, and the system mission or purpose at the bottom right. It includes nodes and links. Nodes are nouns. Links are verbs. A systemigram is read by focusing on a noun that is part of a system and following the links from it, reading the verbs to understand the relationships between system components. Figure 3 is an example of how the concept of security may be modeled using a systemigram.

The systemigram in Figure 3 shows that security may be modeled in terms of its conceptual components. A systemigram has a "mainstay" thread. The mainstay may be viewed as the main thing a system must do in order to be the system named. This is a high level process that is generally agreed by those who understand the system. It is a valid definition in that the layman who encounters the system believes it to be true, and so it has face validity [24]. This is a reasonable place to start in the application of SSM.

Figure 3: Security Systemigram Mainstay

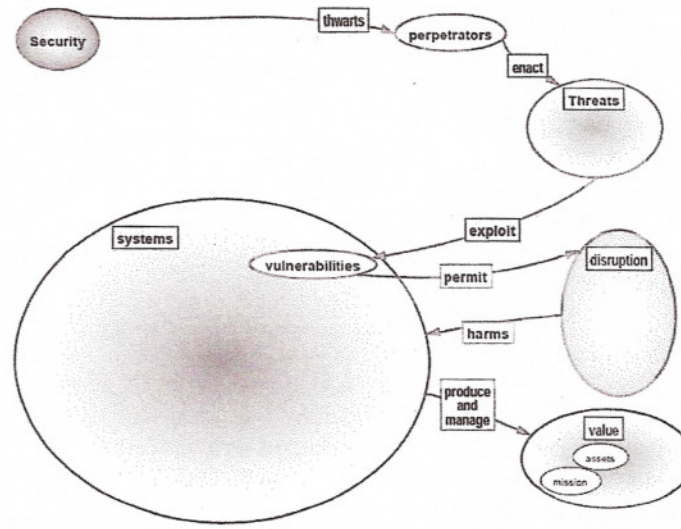
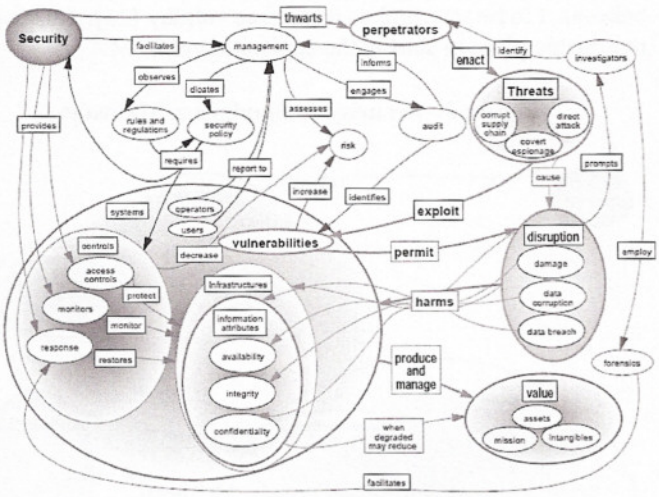


Figure 4 shows the mainstay in the context of various other perspectives on security. Other threads describe actions taken by the system that, though not central to its purpose, are nevertheless associated with any system so named. A systemigram does not produce a single paragraph of text, many of its threads skirt around its subject in an effort to add dimensions to the definition. Each set of noun-verb combinations link the concept to be defined to the object of its actions. The mainstay thread may be viewed as the core definition. But there is no assumption that the mainstay can stand on its own.

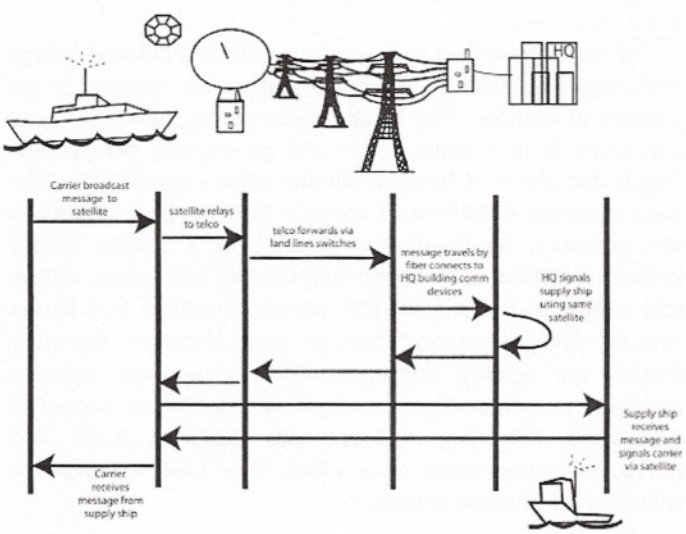
The mainstay thread in Figure 4 is bold and colored orange to distinguish it from other threads that are incorporated in the concept of security. The black cluster shows how security is conceived from a management and governance perspective. The fushia shows it from an administrator's perspective. The most common definition of security that has face validity is the mainstay, which depicts security as a system whose primary function is to thwart perpetrators who enact threats that exploit vulnerabilities that permit disruption that harms systems that produce and manage value. However, the other threads are equally important. Security is also critically necessary to enforce any type of governance. It is composed of prevention, detection, and response methods, tools, and processes that preserve asset value. It is used to authorize access to information resources.

Figure 4: Full Security Systemigram



In order to use a systemigram to model a security standard, we will have to break it down into conceptual components. Those that are common to the standard will be identified The result is that systems security will be characterized orthogonally. Starting with the building blocks for systemic security, we can demonstrate that the extent to which a system may be assessed by comparison with the model. For example, consider the systems architecture and information flow sequence diagram of Figure 5 as an example system. System components in our example system are ship radios, satellites, land-based telecommunications switches, and fiber-connected communications devices. The message sequence diagram of Figure 5 shows how these subsystems support various components of the information flow.

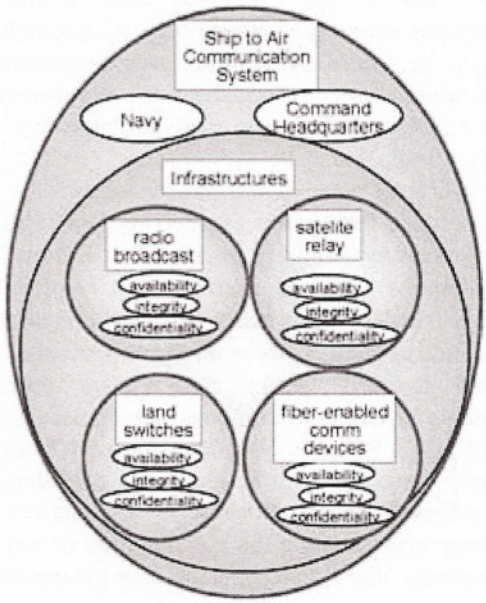
Figure 5: Example System



We compare this system to the foundational concept of security in Figure 4 and we create a new security systemigram using detailed attributes of the target system using the security standard as a metaphor (see Figure 6). We start the comparison by focusing on observable attributes of the systems environment that correspond to the system node in the security systemigram. This example illustrates that the basic information we need to get started is the organizational ownership, management, and infrastructure of each system in the information flow.

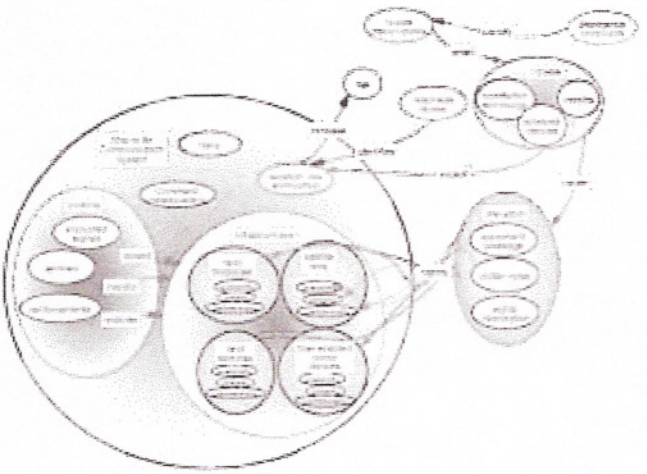
Note that this is not a process to make sure that there are security requirements for every place on each subsystem, which would be an exercise that reduces to a checklist approach to security. Instead, we continue to follow the links that influence the confidentiality integrity and availability requirements backward through the security systemigram and map what we find there to known attributes of our target system.

Figure 6: Systemigram of Example System



For example, in Figure 7 we see that, from what we know about our target system, it has infrastructure containing information in four places, and these are protected by access controls. System confidentiality, integrity, and availability requirements provide observable aspects of security that are easily recognizable cognitive content for systems engineers. Continuing through the security definition build process for our example system, we next consider whether it is possible to account for the potential impact of damage, data corruption, and data breach. Figure 7 illustrates how our model of a security standard in Figure 4 allows us to apply the standard to the target system. Whether or not the standard is useful in adequately securing the system can be inferred by the extent to which systemic security requirements are covered by the mapping exercise.

Figure 7: Example System



IV. Conclusion

This paper provides a definition of security and shows how model-based security may be used in the evaluation of security standards. It describes the results of the first research task in a larger systems engineering security roadmap [25].

These diagrams are currently too high level to completely cover the standard, but they are examples of a systemic media approach to an appropriate solution. Starting with a model of the security standard at a high level allows a fill-in-the-blank approach to identifying where each section or directive in the standard makes sense to compare with the system of interest. It is expected that certain standards will model well to systems with specific characteristics but that no standard will fully cover security requirements of all systems. A complete model of a standard may also identify statements and directives that have no application in any sampled system.

This study is important precisely because it has never been done. Security standards to date have been composed by consensus based on examples of organizations who have compiled security controls in response to known threats. The compositional approach has widespread adoption due to industry consensus rather than due to any attempts at academic justification. Our study will look holistically at a standard. It will also look holistically at system goals for security. Argument and fact-based analysis using systems thinking will be the basis for evaluating the utility of a standard or a given control within a standard. This study will also undoubtedly identify patterns of security features that are similar across systems in different domains. It may result in a systems engineering model for security.

There are a wide variety of uses that a systems engineering may have for the security systemigram. If consensus around standards could be developed, it may be used as a ruler by which to measure whether a system is secure. It may serve as an investigation gathering tool by which to produce requirements. But these uses are premature at present as it is currently a strawman definition. Metrics and requirements would presumably be two of many interrelated domains of research that would benefit by the academic community's consensus on a definition of security.

Acknowledgment

The author is indebted to the influence of Brian Sauser and John Boardman, who have promoted and mentored this systems thinking approach to security.

References

[1] Center for Internet Security, "Information Security Benchmarks and Metrics, cisecurity.org."

[2] Federal Financial Institutions Examination Council, "IT Examination Handbook - Information Security Booklet," ed, 2006.

[3] BITS. *Financial Information Shared Assessments Program.* Available: www.bits.org http://www.sharedassessments.org/

[4] Information Security Forum, "The Standard of Good Practice for Information Security," ed, 2007.

[5] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Information security risk management (ISO/IEC 27005)," ed, 2008.

[6] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Code of practice for information security management (ISO/IEC 27002)," ed, 2005.

[7] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2005, *Information technology — Security techniques — Information security management systems —Requirements (ISO/IEC 27001).* Available: www.iso.org

[8] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques —Information security management — Measurement (ISO/IEC 27004)," ed, 2009.

[9] Information Systems Audit and Control Association, "Control Objectives for Information Technology (COBIT)," ed. Rolling Meadows, IL: IT Governance Institute, 2007.

[10] R. Ross, *et al.*, "Recommended Security Controls for Federal Information Systems, SP 800-53 Rev 2," National Institute of Standards and Technology, Ed., ed, 2007.

[11] B. M. Horowitz, "Frameworks to Guide Cyber Security Solution Application on a Systems Engineering Basis," presented at the Systems Engineering Research Center (SERC) Security Workshop, Washington, D.C., 2010.

[12] C. Woody, "Applying OCTAVE: Practitioners Report," Software Engineering Institute, Carnegie Mellon University CMU/SEI-2006-TN-010, 2006.

[13] INCOSE, "INCOSE Systems Engineering Handbook, Version 3," ed, 2007.

[14] Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems (800-37 Rev1 FINAL DRAFT)," National Institute of Standards and Technology, Ed., ed, 2009.

[15] J. Bayuk, "Information Classification," in *Enterprise Information Security and Privacy*, C. W. Axelrod, *et al.*, Eds., ed: Artech House, 2009, pp. 59-69.

[16] C. Herley, "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," presented at the New security paradigms workshop, Oxford, United Kingdom, 2009.

[17] Information Technology Process Institute, "Visible Ops Handbook and IT Controls Performance Benchmark - fix security reference," 2008.

[18] G. McGraw and B. Chess, "The Building Security In Maturity Model," presented at the Metricon 4.0, Montreal, Canada, 2009.

[19] J. Altmann, "Observational study of behavior: sampling methods," *Behavior*, vol. 49, pp. 227-67, 1974.

[20] P. Checkland, "Soft systems methodology: a thirty year retrospective," *Systems Research and Behavioral Science*, vol. 17, 2000.

[21] P. Senge, *The 5th Discipline, The Art & Practice of the Learning Organization*: Doubleday, 1990.

[22] P. Checkland and M. Winter, "Process and content: two ways of using SSM," *Journal of the Operational Research Society (2006)* vol. 57, pp. 1435–1441, 2006.

[23] J. Boardman and B. Sauser, *Systems Thinking: Coping with 21st century problems*: Taylor & Francis, 2008.

[24] B. Nevo, "Face Validlity Revisited," *Journal of Educational Measurement,* vol. 22, pp. 287-293, 1985.

[25] J. Bayuk, et.al.,, "Systems Security Engineering Roadmap, Final Technical Report," Systems Engineering Research Center (SERC UARC) SERC-2010-TR-005, 2010.

Jennifer L. Bayuk (M'08) is the Cybersecurity Program Director of the School of Systems and Enterprises at Stevens Institute of Technology. She develops graduate curriculum for security systems engineering and enterprise security architecture, as well as leading research in systems security engineering. Bayuk has been a Wall Street Chief Information Security Officer, a Manager of Information Systems Internal Audit, a Price Waterhouse Security Principal Consultant and Auditor, and a Security Software Engineer at AT&T Bell Laboratories. Bayuk frequently publishes and speaks on IT Governance, Information Security, and Technology Audit topics.

She is the author of *Stepping Through the IS Audit, 2nd Edition* (ISACA2004), *Stepping Through the InfoSec Program* (ISACA 2007), and Enterprise Security for the *Executive* (Praeger, 2010). She also has co-edited a collection of works on enterprise information security and privacy.

Ms. Bayuk is a Certified Information Security Manager, a Certified Information Systems Security Professional, a Certified Information Security Auditor, and Certified in the Governance of Enterprise IT (CISM, CISSP, CISA, and CGEIT), as well as a member of IEEE, INCOSE, and ACM. She has Masters Degrees in Computer Science (SIT) and Philosophy (OSU).