CYBER SECURITY POLICY GUIDEBOOK

JENNIFER L. BAYUK
JASON HEALEY • PAUL ROHMEYER
MARCUS H. SACHS • JEFFREY SCHMIDT • JOSEPH WEISS

WILEY

Cyber Security Policy Guidebook

Cyber Security Policy Guidebook

Jennifer L. Bayuk
Independent Cyber Security Governance Consultant
Industry Professor at Stevens Institute of Technology, Hoboken, NJ

Jason Healey
Director of the Cyber Statecraft Initiative
Atlantic Council of the United States, Washington, D.C.

Paul Rohmeyer
Information Systems Program Director
Howe School of Technology Management
Stevens Institute of Technology, Hoboken, NJ

Marcus H. Sachs
Vice President for National Security Policy
Verizon Communications, Washington, D.C.

Jeffrey Schmidt
Chief Executive Officer
JAS Communications LLC, Chicago, IL

Joseph Weiss
Professional Engineer
Applied Control Solutions, LLC, Cupertino, CA

A John Wiley & Sons, Inc., Publication

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Cyber security policy guidebook / Jennifer L Bayuk ... [et al.].
p. cm.
Summary: "This book is a taxonomy and thesaurus of current cybersecurity policy issues, including a thorough description of each issue and a corresponding list of pros and cons with respect to identified stances on each issue" – Provided by publisher.
ISBN 978-1-118-02780-6 (hardback)
1. Information technology–Government policy. 2. Computer security–Government policy. 3. Data protection–Government policy. I. Bayuk, Jennifer L.
QA76.9.A25C91917 2012
005.8–dc23

2011036017

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Foreword

Not long ago, I was the Director of Cybersecurity Policy at the U.S. Department of Homeland Security (DHS). In that role, I routinely met with the department's staff responsible for cyber security operations. In one such meeting, focused on cyber risk management and metrics, we were having a bit of a difficult time seeing one another's perspectives on a related issue. At one point a senior member of the operations staff looked across the table at me and opined, "You actually think policy ought to drive operations?"

Beyond the obvious dysfunction behind his question, it pointed to some of the core themes this book attempts to address: cyber security policy's importance, its relation to both strategy and operations, its relevance to a very diverse set of stakeholders and decision makers, and the inevitable controversy and debate it engenders. These are very much the issues of our time, but they are not issues for the timid.

Perhaps to my DHS colleague's chagrin, in fact, policy does and should drive operations. As the authors clearly point out, policy necessarily drives decisions at many different levels. How many of us have not heard the President of the United States include these words in a speech, "it is the policy of my administration. . . ."? His job is (with Congress) to set national policy, approve appropriate implementation activities to carry out that policy, and then ensure that policy is properly enforced or adjusted as circumstances dictate. Executives at other levels have similar responsibilities.

In the evolution of all things cyber, however, policy has not been a driver. Rather, it has been an afterthought. The authors make this very point in several ways, and in so doing, they raise a vitally important issue: should cyber security policy always be reactive? The obvious answer is "no;" or else the operations and standards it drives will also always be reactive, leading to an inherently untenable situation in which cyber security efforts always lag the attacks they are meant to prevent. If this situation sounds

all too familiar, it is because cyber security practitioners have been on this treadmill far too long, with no sign of it ending.

The great problem, of course, is that the setting of proactive cyber security policy is, at least in any democratic environment, an extremely difficult and time-consuming task. Even the simplest perusal of Chapter 6 of this book will be sufficient to inform the reader that the ground on which almost any cyber security policy is contested is muddy ground indeed.

As a general rule, when one is most muddled with the complexity of building a particular system correctly, it is best to take a big step back—and then elevate oneself to see the larger picture. Only then can one ask the all-important question framed in this book, "Am I building the right system?" In my own experience, the too frequent answer to this question is "no." It is incredibly painful for those who are building the wrong system, but building it correctly, and therefore deeply invested in it, to hear that answer.

All of which points, I believe, to the raison d'etre for a *Cyber Security Policy Guidebook* such as this. If read with an unjaundiced eye, it will help the reader to see the bigger cyber security picture and its vitally important policy setting, no matter the vantage point. This cannot help but be an aide.

It is a very happy circumstance that the authors of this book are highly regarded professionals, experts in their respective niches, and that they bring many years of experience to the topic. As they point out, the topic is incredibly expansive—a natural result of the ubiquity of "cyber" anything in today's networked world. Indeed, if the topic were not so incredibly important and relevant, it might be silly even to attempt to get one's arms around it.

But to anyone for whom national security, business operations, or anything related to the Internet is important, and that covers most of us, understanding some measure of the topic is critical. To that end, this book is most useful.

Andy Cutts
Former Director of Cybersecurity Policy
at the U.S. Department of Homeland Security

Preface

The idea for this book coincided with a conference on Cyber Security Policy (SIT 2010). The conference had sessions ranging from security technology investment decisions by venture capitalists to the implications of cyber security policy on personal privacy. Though all speakers were experts in their field and were asked to address cyber security policy topics, many instead focused on strategy or technology issues. Even where it was clear that policy was being discussed, policies were often not articulated clearly enough for panelists and audience members to participate in informed debate. This observation itself became the buzz at the conference and made it a truly memorable experience for many who attended.

The experience made it clear that cyber security policy means different things to different people, even those who work in cyber security. This conclusion led us to the format of this book. That is, the book is designed to lead the reader through concepts that are individually easy to assimilate, and collectively provide a solid understanding of the field of cyber security and the place of policy within it.

We also knew that there is no one person experienced enough in cyber security to have been able to single-handedly write this book. The team was chosen to ensure that all the major fields of experience in cyber security were covered. Each contributed to chapters and sections that were specific to their experience. However, all chapters were scrutinized by all authors to ensure a cohesive presentation for the expected variety of readers. Policy is the domain of authoritative executives. Executive authority may stem from the social contracts by which governments are established or the domain of a private enterprise. This book was written with those executives in mind, but it is not intended solely for their consumption. In order that cyber security policy analysis receive the critical scrutiny essential to sound legislation on both public and private fronts, the audience for this book must extend to executive advisors, educators,

researchers, legislative staff, and practitioners in the field. Though each member of the audience brings his or her own background and experience to the material presented herein, we expect that current concepts on cyber security policy will be enriched by sharing this common presentation framework and nomenclature with colleagues in the same field, whose professional experience has exposed them to cyber security issues of varying scope. Most literature about cyber security falls into two categories: technology and advice. This book will refrain from technical jargon and also from recommendations with respect to decisions in any given case of cyber security policy. Although the book endeavors to explain technology issues in cyber security, it does so in layman's terms. At the same time, the book emphasizes the importance of critical and analytical thinking about decisions with respect to cyber security and will equip the reader with descriptions of the impact of specific policy choices, letting the reader decide whether to view that impact as positive or negative.

This guidebook integrates explanations of cyber security policy alternatives across potential executive, legislative, judiciary, commercial, military, and diplomatic action. Readers across these disciplines are expected to view its contents through the lens of their own area of expertise and also gain insights from issues encountered by others. It will be an introductory text for the uninitiated, while at the same time providing a holistic reference for experts in the field of cyber security.

Originally, the outline of the book was divided into policy domains as defined in the conference, and from these were created book sections assigned to each author. Once work began, however, there was immediate skepticism and doubt among the authors on the approach. Some topics at the conference were broad in scope. For example: *Law Enforcement, Privacy, Civil Rights, and Personal Liberties*; *Emergent Technologies, Innovation, and Business Growth*; and *Global Implications of Cyber Security Policies*. Others were focused on a specific type of system, such as *Next Generation Air Transportation System* and *Electric Power Distribution*. No one thought that simply combining policy content from each section would achieve the mission of the volume. The volume could not appear splintered into sets of issues of interest to only one industry while still achieving its goal of educating an outsider on what a cyber security policy issue was. This recognition led to the development of a more holistic, unified view of the guidebook approach.

Chapter 1 introduces the reader to the relationship between cyberspace, cyber security, and cyber security policy. Chapter 2 provides a brief history of cyber security. It provides the background necessary for a lay person to understand the current state of the art as well as the state of the practice in establishing security controls in cyberspace. The chapter is not a chronicle of cyber crime or legislative attempts to establish cyber security controls, but it does highlight significant events that have influenced the evolution of controls.

Chapter 3 describes the state of the practice in measuring cyber security. It revisits the history of Chapter 2 from the perspective of security goals and objectives. It discusses various approaches that have been used to determine whether goals for cyber security have been met. Three case studies of cyber-enabled systems illustrate the approaches. The case studies are of e-commerce, industrial control systems, and personal mobile devices.

Chapter 4 provides guidance for executive decision makers charged with large organizations or constituencies that are cyber security stakeholders. It emphasizes that cyber security management is not unlike other management activities in that successful execution requires clearly articulated goals and corresponding program management. It provides an outline of how to begin to establish a cyber security strategy and associated cyber security policy effort. It suggests a perspective on cyber security issues that is integrated with the mission and purpose of the organization.

Chapter 5 introduces a catalog approach to the examination of cyber security policy issues. It places the history of cyber security and metrics of Chapters 2 and 3 against the context of cyber operations in order to separate the security issues into areas of responsibility. The word "policy" in the domain of cyber security applies to different dimensions of societal issues across multiple organizations and industries. Hence, Chapter 5 describes a demarcation in the scope of issues faced by decision makers in different positions of influence. That is, the policy decisions faced by a telecommunications executive will be very different from the policy decisions faced by a military strategist. However, these divisions are purposely described in chapter sections and not as domains of influence or responsibility because they significantly overlap. The division is made to enhance clarity of explanation and is not meant to introduce nonexistent boundaries.

Chapter 6 builds on the concepts and definitions described in Chapters 1 to 5 to explain the cyber security environment faced by decision makers in each of the five sections of cyber security policy that were introduced in Chapter 5. Each section includes a list of cyber security policy issues faced by different organizations and industries who are stakeholders.

Chapter 7 chronicles the efforts of the U.S. government to align cyber security strategy and policy and observes the impact of historical events on cyber security policy. It closes with references to literature that suggest alternative courses forward.

Chapter 8 presents a summary and shows how the content of each chapter presents different perspectives on the same topic, which is cyber security policy. It emphasizes that approaches to cyber security policy are necessarily different for different cyberspace stakeholders and that the value of security measures must be weighed against their efficacy in achieving individual cyberspace strategy objectives.

We are all five left with a deep appreciation for the depth and breadth of our adopted field. Marcus Sachs' first-hand experience in both the public

and private policy arena was invaluable when it came to chronicling history. Jason Healey's wealth of experience in policy analysis in both government service and private research shed light on a rich array of issues in nation-state and global diplomacy. Joe Weiss' in-depth expertise in industrial control systems prevented us from losing focus on critical attributes of our technology infrastructure. Paul Rohmeyer's academic and business experience in technology management consistently made sure that our narratives were not only meaningful to decision makers, but also that the whole carried a strategic purpose that was obvious to our target audience. Jeff Schmidt's career-long immersion in Internet governance and software engineering issues provided a sound sanity check on completeness. Jennifer Bayuk's solid technical background and layman-accessible writing skills framed the presentation of concepts that made sense of it all.

Together, we dedicate this volume to cyber security policymakers, whether vocal or silent. May you achieve success in your respective missions.

Jennifer L. Bayuk
Jason Healey
Paul Rohmeyer
Marcus H. Sachs
Jeffrey Schmidt
Joseph Weiss

Acknowledgments

This book was inspired by the Honorable Mike Wynne, the 21st Secretary of the Air Force, who established considerable capability for cyber security in the Air Force, and was at the time single-handedly responsible for raising the awareness of national security-related cyber security policy issues. Among countless other laudatory and critical advisory appointments, Mr. Wynne serves as the Chair of the Advisory Board for the Systems Engineering Research Center and also as Senior Advisor to the President at Stevens Institute of Technology.

To create awareness within academia of the importance of cyber security policy, Mr. Wynne chaired a conference on that topic sponsored by Stevens Institute of Technology (SIT 2010). Opinions were solicited from experts in a wide variety of fields who are stakeholders in cyberspace. Many of them spoke at the conference or attended the discussions. Some were unable to attend but provided their comments in written form. Our grateful thanks extend to the speakers and other participants who lent their expertise to that conference.

We are most indebted to those who reviewed the first completed drafts of this volume. Their invaluable feedback has considerably enhanced the comprehensibility of the cyber security policy curriculum contained herein. We therefore gratefully acknowledge these individuals for their efforts and expertise: Warren Axelrod, Larry Clinton, Kevin Gronberg, Richard Menta, William Miller, Brian Peretti, Andy Purdy, and Michael zur Muehlen. Others who spoke or sent material to be included in this book are also gratefully acknowledged. They include: Michael Aisenberg, Edward Amoroso, Tom Arthur, Paige Atkins, James Arden Barnett, John Boardman, David M. Bowen, Christopher Calabrese, Ann Campbell, C. R. Collazo, Greg Crabb, William Crowell, Matthew D. Howard, John A. Davis, Christopher Day, James X. Dempsey, Edward C. Eichhorn, Robert Elder, Steve Elefant, Dan Geer, Charles Gephart, Gary Gong, Gail L. Graham, Kevin Harnett, Melissa Hathaway, Husin bin Hj Jazri, Erfan Ibrahim, Robert

R. Jueneman, Jeffrey S. Katz, John Kefaliotis, Alan Kessler, George Korfiatis, Darren Lacey, Pascal Levensohn, Martin Libicki, Chan D. Lieu, Eric Luiijf, Pablo Martinez, Douglas Maughan, Ellen McCarthy, Dale Meyerrose, Gregory T. Nojeim, John Osterholz, James B. Peake, Jim Richberg, Robert D. Rodriguez, Tom Ruff, Brian Sauser, Ted Schlein, Agam Sinha, Ben Stewart, John N. Stewart, Eric Trapp, David Weild, John Weinschenck, and Paul Winstanley. We have incorporated as many opinions as possible from that conference. We are grateful to these experts for sharing their insight. We look forward to continuing the cyber security policy debates in a constructive manner that will secure peace and prosperity in cyberspace going forward.

1

Introduction

1.1 What Is Cyber Security?

Cyber security refers generally to the ability to control access to networked systems and the information they contain. Where cyber security controls are effective, cyberspace is considered a reliable, resilient, and trustworthy digital infrastructure. Where cyber security controls are absent, incomplete, or poorly designed, cyberspace is considered the wild west of the digital age. Even those who work in the security profession will have a different view of cyber security depending on the aspects of cyberspace with which they personally interact. Whether a system is a physical facility or a collection of cyberspace components, the role of a security professional assigned to that system is to plan for potential attack and prepare for its consequences.

Although the word "cyber" is mainstream vernacular, to what exactly it refers is elusive. Once a term of science fiction based on the then-emerging field of computer control and communication known as cybernetics, it now refers generally to electronic automation (Safire 1994). The corresponding term "cyberspace" has definitions that range from conceptual to technical, and has been claimed by some to be a fourth domain, where land, sea, and air are the first three (Kuehl 2009). There are numerous definitions of cyberspace and cyber security scattered throughout literature. Our intent is not to engage in a debate on semantics, so we do not include these definitions. Moreover, such debates are unnecessary for our purpose, as we generally use the term "cyber" not as a noun, but as an adjective that modifies its subject with the property of supporting a collection of automated electronic systems accessible over networks. As well reflected in

Cyber Security Policy Guidebook, First Edition. Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss.

language-usage debates in both the field of cognitive linguistics and popular literature on lexicography, the way language is used by a given community becomes the de facto definition (Zimmer 2009), and so we request that our readers set aside the possibility that they will be confused by references to "cyberspace" and "cyber security" and simply refer to their own current concept of these terms when it makes sense to do so, while keeping in mind that we generally the term cyber as an adjective whose detailed attributes will change with the system of interest.

At a high level, cyber security is typically explained in terms of a few triads that describe the objectives of security professionals and their methods, respectively (Bayuk 2010). Three that combine to cover most uses of the term are:

- *prevent, detect, respond*
- *people, process, technology*
- *confidentiality, integrity, and availability*.

These reflect the goals of cyber security, the means to achieve cyber security, and the mechanisms by which cyber security goals are achieved, respectively.

Prevent, detect, respond addresses goals common to both physical and cyber security. Traditionally, the primary goal of security planning has been to prevent a successful adversary attack. However, all security professionals are aware that it is simply not possible to prevent all attacks, and so planning and preparation must also include methods to detect attacks in progress, preferably before they cause damage. However, whether or not detection processes are effective, once it becomes obvious that a system is threatened, security includes the ability to respond to such incidents. In physical security, the term "first responders" refers to the heroic individuals in policy, fire, and emergency medical professions. Response typically includes repelling the attack, treating human survivors, and safeguarding damaged assets. In cyber security, the third element of the triad is often stated in slightly more optimistic form. Rather than "respond" it is "recover" or "correct." This more positive expectation on the outcome of the third triad activity, to recover rather than simply respond, reflects the literature of information security planning, wherein security management is recommended to include complete reconstitution and recovery of any business-critical system. Because information technology allows diversity, redundancy, and reconstitution for the data and programs required to operate systems, information security professionals expect that damage can be completely allayed. In either case, the lessons learned in response are expected to inform prevention planning, creating a loop of continuous security improvement.

People, process, technology addresses methods common to both technology management in general and to cyber security management as a specialized field. This triad observes that systems require operators, and

operators must follow established routines in order for systems to accomplish their missions. When applied to security, this triad highlights the fact that security is not achieved by security professionals alone, and also that cyber security cannot be accomplished with technology alone. The system or organization to be secured is acknowledged to include other human elements whose decisions and actions play a vital role in the success of security programs. Even if all these people had motivation and interest to behave securely, they would individually not know how to collectively act to prevent, detect, and recover from harm without preplanned process. So security professionals are expected to weave security programs into existing organizational processes and make strategic use of technology in support of cyber security goals.

Confidentiality, integrity, and availability addresses the security objectives that are specific to information. Confidentiality refers to a system's capability to limit dissemination of information to authorized use. Integrity refers to ability to maintain the authenticity, accuracy, and provenance of recorded and reported information. Availability refers to the timely delivery of functional capability. These information security goals applied to information even before they were on computers, but the advent of cyberspace has changed the methods by which the goals are achieved, as well as the relative difficulty of goal achievement. Technologies to support confidentiality, integrity, and availability are often at odds with each other. For example, efforts to achieve a high level of availability for information in cyberspace often make it harder to maintain information confidentiality. Sorting out just what confidentiality, integrity, and availability means for each type of information in a given system is the specialty of the cyber security professional. Cyber security refers in general to methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace.

1.2 What Is Cyber Security Policy?

Cyber has created productivity enhancements throughout society, effectively distributing information on a just-in-time basis. No matter what industry or application in which cyber is introduced, increased productivity has been in the focus. The rapid delivery of information to cyberspace often reduces overall system security. To technologists engaged in productivity enhancements, security measures often seem in direct opposition to progress due to prevention measures that reduce, inhibit, or delay user access, detection measures that consume vital system resources, and response requirements that divert management attention from system features that provide more immediately satisfying system capabilities. The tension between demand for cyber functionality and requirements for security is addressed through cyber security policy.

The word "policy" is applied to a variety of situations that concern cyber security. It has been used to refer to laws and regulations concerning information distribution, private enterprise objectives for information protection, computer operations methods for controlling technology, and configuration variables in electronic devices (Gallaher, Link et al. 2008). But there is a myriad of other ways in which literature uses the phrase *cyber security policy*. As with the term "cyberspace," there is not one definition, but there is a common theme when the term *cyber security* is applied to a policy statement as an adjective. The objective of this guidebook is to provide the reader with enough background to understand and appreciate the theme and its derivatives. Those who read it should be able to confidently decipher the numerous varieties of cyber security policy.

Generally, the term "cyber security policy" refers to directives designed to maintain cyber security. Cyber security policy is illustrated in Figure 1.1 using a modeling tool that is used to make sense of complex topics called a systemigram (Boardman and Sauser 2008). A systemigram creates an illustrative definition succinctly by way of introducing components of the thing to be defined (all nouns) and associating them with the activity they generate (all verbs). The tool requires that all major components be connected via a "mainstay" that links the concept to be defined (top left) to its

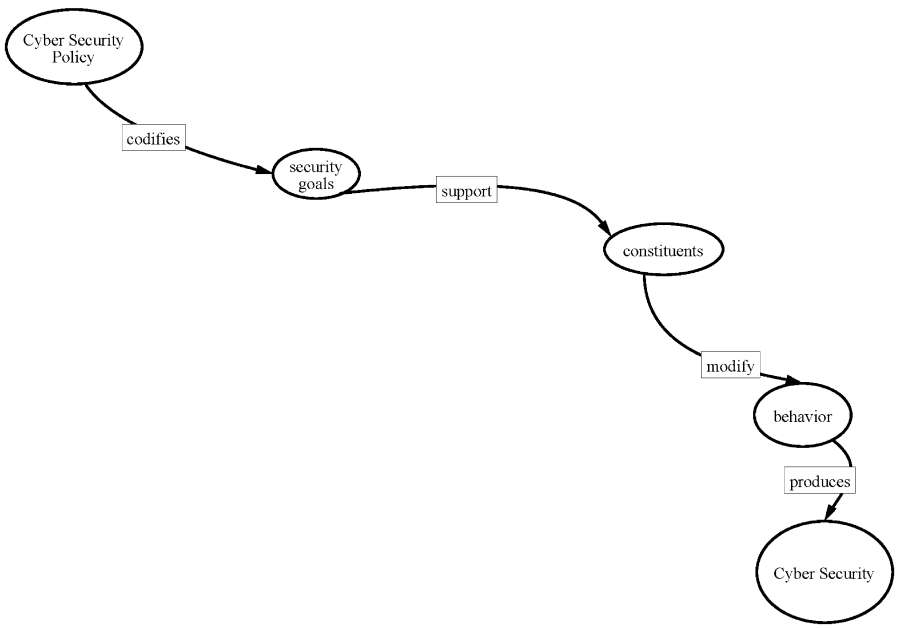

Figure 1.1 Cyber security policy definition.

purpose or mission (bottom right). The mainstay is expected to capture the layman's view of the concept. Other perspectives on the concept to be defined may be represented as supplementary perspectives on the complex concept.

In Figure 1.1, cyber security policy is presented as something that codifies security goals in support of constituents who are expected to modify their behavior in compliance with the policy to produce cyber security. Figure 1.2 fleshes out the concept, adding the color of different perspectives on cyber security policy. Although not all the additional nodes and links are strictly within the scope of a definition of cyber security policy, they provide insight into the scope as defined in the mainstay of the systemigram of Figure 1.1.

In Figure 1.2, the links to and from the "governance bodies" node illustrate that cyber security policy is adopted by governing bodies as a method of achieving security goals. The figure is purposely generic as governing bodies often exist outside of the organizations that they govern. For example,

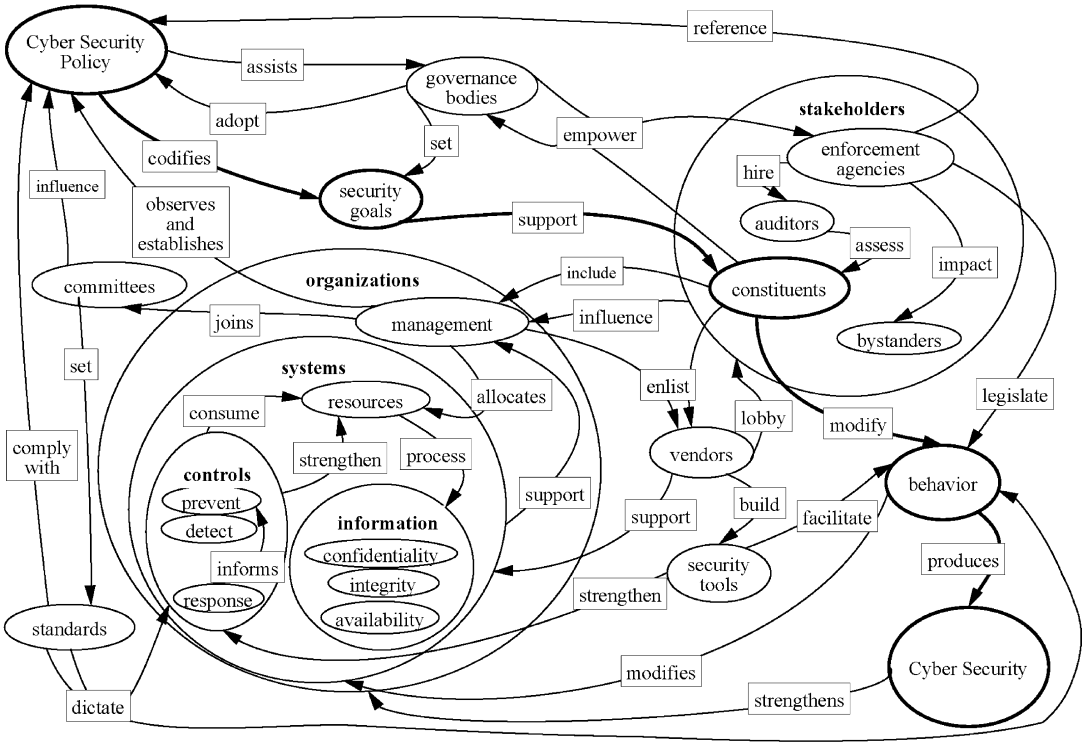

Figure 1.2 Cyber security policy perspectives.

a nation-state may be a governing body, but one may also consider a centralized corporate security office a governing body over multiple independent business units. The links emanating from the "enforcement agencies" node illustrate the role of policy enforcement agencies, who establish laws, rules, and/or regulations that are meant not only to affect constituent behavior, but also affect others, who thereby become stakeholders in the policy process. The links on the far left acknowledge the role of standards that are set by management of organizations who are bound by the governing bodies to comply with policy. The links emanating from the node labeled "vendors" depicts the vendor relationships of constituents and management, who both influence and are influenced by vendors who provide tools for security policy compliance and support systems security with products and services.

The clusters of nodes and links within and adjoining the "organizations" node refer to an organization that is subject to policy. It shows that such organizations observe cyber security policies issued by governing bodies as well as establish their own internal cyber security policies. It also illustrates that organizational management is both supporting and is being supported by systems that are impacted by security policy. The "systems" node refers to the systems used to operate cyberspace, highlighting the interdependent relationship between security controls and system resources. It shows that there is a trade-off between systems resources devoted to security controls and those required to process information; that is, the more security control processes can be integrated into systems operation, the less of a resource drain security will be. A typical goal in an internal organizational cyber security strategy is to optimize this trade-off, using documented policy as a communications tool to create awareness that such decisions have been made.

Note that, as illustrated in Figure 1.2, the role of policy is to provide a foundation upon which to prescribe rules for behavior that are expected to achieve cyber security. There is a wide variety of cyber domains that will have vastly different policy statements and associated rules. These domains are further described in Chapter 6. Goals for cyber security do not directly translate into behavior, but a cyber security strategy based upon cyber security goals is expected to culminate in better cyber security policy. Organizations create standards for implementing technology controls and related operational processes and constituents use these standards to comply with policy. Standards are not themselves policies. Rather, they are translations from policy objectives onto a set of technologies and operational processes. Where a standard is directed at policy compliance, it specifies a combination of process and technology configuration that will achieve policy compliance. However, standards may be issued that are not directed at any specific policy objective, and policies may lack corresponding standards.

1.3 Domains of Cyber Security Policy

As depicted in Figure 1.2, cyber security policy is adopted by a governing body and formally applies only to the corresponding domain of governance. The constituents of a security policy, who may also be considered stakeholders, will vary with the scope of the policy. For example, a nation-state cyber security policy will encompass all citizens and perhaps foreign businesses operating within its domain, whereas a corporate cyber security policy will apply only to staff with which the corporation has employment or other legal agreements which may reasonably be expected to motivate behavioral modification. Even suppliers who are wholly dependent on a single customer cannot be expected to conform to that customer security policy unless under a contractual obligation to do so. The content of security policy will change with the goals of the corresponding governing body. The goals of nation-state security are very different from the goals of corporate security, and so policy statements and corresponding expected activities in support of policy will appear very different.

The way policy is compiled, documented by enforcement agencies, and ratified will also differ with its corresponding governing body and constituency. In government, the process by which goals are codified into policy and the process by which policies are codified into legislation are separate and distinct processes. However, in corporations, it is common to have one central security department responsible for both the cyber security policy and the associated standards and procedures which are the corporate equivalent of regulatory guidance.

Where security is a priority for an organization, it is common to see cyber security policies issued by multiple internal departments with overlapping constituencies, who then sometimes detect policy incompatibility issues in trying to follow them all simultaneously.

1.3.1 Laws and Regulations

Nation-state cyber security policy is currently considered to be a subset of national security policy. Even if nation-state cyber security policy was considered to be on the same plane as foreign policy or economic policy, these policies do not have the same force as law. Rather, policies are established and articulated through reports and speeches, through talking points and negotiations. Policy is used to guide judgment on what laws and regulations to consider. It does not refer to the laws and regulations themselves. Of course, in the best of all possible worlds, treaties, laws, and regulations would reflect a wise and thoughtfully conceived policy. Nevertheless, it is possible to have cyber security executive directives, laws, and regulations without having articulated a cyber security policy at all.

For example, China has clearly established a policy that cyberspace activities critical to nation-state operations shall be controlled (Bishop 2010). This policy states clearly that the Internet shall serve the interests of the economy and the state. The policy has led to laws and regulations that allow the Chinese government to segregate, monitor, and control telecommunications facilities as well as block access to Internet sites they identify as contrary to their interests.

In the United States, by contrast, most laws and regulations that impact cyber security were not developed specifically to address issues of cyberspace, but have emerged as relevant to cyber security in the context of policy enforcement. The policy is often economic in nature. For example, any financial institution that is regulated by the Office of the Comptroller of the Currency has been subject to security audits and assessments of their Internet-facing infrastructure. A 2009 U.S. Cyber Security Policy Review actually redefined the word policy: "Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (Hathaway et al. 2009). This is the full range of issues to be considered when developing security policy. Moreover, the result of this review was not a policy recommendation. It simply outlined a strategy for ongoing communications and cooperation between the public and private sector with the goal of increasing national resilience to cyber attack. The U.S. approach to cyber security policy will be further discussed in Chapter 7.

Whether or not a government cyber security policy is articulated, its cyber security rules will be limited to the scope of its governance domain. That is, a branch or agency of a government will be within the scope of, and thus subject to, any government-wide regulation, so its own policy and rules must be consistent with that broader scope. A branch or agency will only be able to create new legislation for its own constituency and within its own charter. For example, cyber security policy issued by an industry regulator will apply only to those industries in its regulatory domain. An energy regulator will be able to require an energy facility to have redundant communications, but it will not be able to require that telecommunications providers lay redundant cables to each energy facility. Only a telecommunications industry regulator may set rules for the telecommunications industry, and the charter is not likely to include services provided to another regulator's domain. Such gaps in a holistic system-level approach to critical infrastructure regulation leave loopholes in the form of constraints that become excuses for partial and inadequate security coverage. To be effective, cyber security policy would have to span mul-

tiple regulatory domains for a single purpose, such as the U.S. Federal Trade Commission.

1.3.2 Enterprise Policy

Private sector organizations are generally not as constrained as governments in turning senior management policies into actionable rules. In a corporate environment, it is typical that policies are expected to be followed upon threat of sanction, up to and including employment termination. For example, human resources, legal, or accounting policies have been codified to the point where any instance of noncompliance may amount to reason for termination. Where mid-level managers support processes such as staff hiring or expense filing, they may be expected to bring department activities into compliance with those policies, and often will have to establish department-level metrics for compliance. As in the case of government, any such suborganization will be subject to constraints of authority in scope. Though there are exceptions in places that take information classification very seriously, a corporation security policy issued by a Chief Executive Officer will generally apply to an entire corporation, but one issued by a Chief Information Officer will typically only apply to the technology staff. A recent change in the organizational landscape is the appointment of a chief information security officer (CISO) or chief privacy officer (CPO) whose is responsible for selected aspects of the organization's security posture. However, the responsibilities in these roles are not as well accepted as those of a Chief Financial Officer (CFO), and sometimes such duties are more about public relations than security management.

An unfortunate difference between most corporate cyber security policies and those issued by a legal or human resource department is that cyber security policies often leave the assessment of cyber security risks to mid-level managers who may not be familiar with cyber security or risk management concepts. By analogy with a CFO policy, this is like leaving the definition of appropriate travel expenses up to the traveler. For example, a cyber security policy may state, "where risk of information confidentiality compromise is high, the information should not be allowed to be shared with a vendor without a duly diligent review of vendor capability to secure information." This type of policy leaves the information risk assessment to a manager who may be motivated to cut costs by outsourcing part of the department information flow. To further reduce those costs, that same manager may decide a due diligence review is not warranted. Such a situation may be caused by the misallocation of security responsibilities to someone who is not qualified, or it may be that the culture of the organization is risk-tolerant, but either way, it presents a segregation of duties issue. These situations are exacerbated by the fact that measures of cyber security are not as mature as metrics in the domains of accounting or human resources. Cyber security metrics are more fully discussed in Chapter 3.

1.3.3 Technology Operations

In an effort to assist clients in complying with legal and regulatory information security requirements, the legal, accounting, and consulting professions have adopted standards for due diligence with respect to information security, and recommended that clients model processes around them. These were sometimes proprietary to the consulting firm, but were often based on published standards such as the National Institute of Standards and Technology (NIST)'s *Recommended Security Controls for Federal Information Systems* (Ross, Katzke et al. 2007) and their private sector counterparts (ISO/IEC 2005a,b; ISF 2007). Where a standard becomes the preferred mode of operation for securing a technology environment, it will often be referred to as a cyber security policy for technology operations and management.

Whether these technology operations policies dictate simply that the standard should be followed, or they customize the standard with specific roles and responsibilities for process execution within the computer operations organization, the scope of the policy will be limited to the management and operations of a well-defined technology platform. It is sometimes even the case that the same organization will run multiple technology platforms, but their cyber security policy will apply only to a subset. This may be the case at a technology services provider who charges extra for security services, so not all of their customers' platforms will be covered by the security policy.

By the strict definition of policy as a high-level management directive, these types of documents may not be considered by all security professionals to be policy at all, but rather processes or standards. However, as the current literature includes this nomenclature, we observe this usage is prevalent. Nevertheless, in this book, we will typically use the term policy to refer to higher level management directives that articulate and codify strategy for overall cyber security goal achievement as opposed to policy for the correct operation of a technology-only process.

1.3.4 Technology Configuration

Because many technology operations standards are implemented using specialized security software and devices, technology operators often colloquially refer to the standard-specified technical configuration of these devices as "security policy." These specifications have over the years been implemented by vendors and service providers, who devised technical configurations of computing devices that would allow system administrators to claim compliance with various standards. This has led vendors to label alternative technical configurations for their products as "security policies." Vendor marketing literature presents these technical configurations as "policy" in an effort to align their solutions with the overall enter-

prise strategy. For example, "our product allows you to automate your enterprise security policy."

Similar to the use of the word policy to refer to operational processes and standards, this use of the word policy does not correspond to management directives for security. But again, as the current literature includes this nomenclature, we observe this usage is prevalent. Usually, this usage of the term policy will appear with an adjective for the device or technology that is configured. For example, the words "firewall policies" or "UNIX security policy" indicate that the object is a set of technical configuration variables rather than a directive by high-level management. These technologies and devices are further discussed in Chapter 2.

1.4 Strategy versus Policy

Cyber security policy articulates the strategy for cyber security goal achievement and provides its constituents with direction for the appropriate use of cyber security measures. The direction may be societal consensus or dictated by a governance body. We also recognize that independent enterprises need to establish management directives in support of cyber security strategy, and we use the modified term, "enterprise policy" to refer to policies that apply only within a given enterprise community. Though such enterprise policy is often guided by standards for cyber security such as those established by the International Organization for Standardization (ISO) (ISO/IEC 2005a,b) and NIST (Ross, Katzke et al. 2007), those standards by themselves are not policies. Such standards typically contain a combination of process guidance with technology control recommendations. The process guidance recommends that policy be established, but cannot by itself properly be called policy.

In the sense that all policies differ from the implementation standards with which they are enforced, policy can be guesswork, because the simple adoption of policy does not guarantee that the right corresponding rules will be established to achieve security goals. Without a clear conceptual view of cyber security influences, it would be difficult to devise cyber security strategy and corresponding policy. Even if there is widespread consensus on the policy enforcement mechanisms, and these can be directly traced to policy directives, the collective judgment could be misguided, and those mechanisms may fail to achieve security policy goals. Chapter 6 provides many examples of policy statements that may have unintended consequences. Key to cyber security policy formulation is (1) to recognize that security control decisions are made regardless of whether there is a formal policy in place, (2) to understand that policy is the appropriate tool to guide multiple independently made security decisions, and (3) to absorb as much information as possible about how security decisions are influenced in the course of devising security strategy.