INTERNAL AUDIT AND IT AUDIT SERIES

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)

Dan Shoemaker • Anne Kohnke • Ken Sigler

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)

Internal Audit and IT Audit

Series Editor: Dan Swanson

PUBLISHED

Leading the Internal Audit Function
by Lynn Fountain
ISBN: 978-1-4987-3042-6

Securing an IT Organization through Governance, Risk Management, and Audit
by Ken Sigler and James L. Rainey, III
ISBN: 978-1-4987-3731-9

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)
by Dan Shoemaker, Anne Kohnke, and Ken Sigler
ISBN: 978-1-4987-3996-2

Operational Assessment of IT
by Steve Katzman
ISBN: 978-1-4987-3768-5

The Complete Guide to CyberSecurity Risks and Controls
by Anne Kohnke, Dan Shoemaker, and Ken Sigler
ISBN: 978-1-4987-4054-8

Software Quality Assurance: Integrating Testing, Security, and Audit
by Abu Sayed Mahfuz
ISBN: 978-1-4987-3553-7

FORTHCOMING

Practical Techniques for Effective Risk-Based Process Auditing
by Ann Butera
ISBN: 978-1-4987-3849-1

Internal Audit Practice from A to Z
by Patrick Onwura Nzechukwu
ISBN: 978-1-4987-4205-4

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)

Dan Shoemaker • Anne Kohnke • Ken Sigler

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20160121

International Standard Book Number-13: 978-1-4987-3996-2 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Shoemaker, Dan, author. | Kohnke, Anne, author. | Sigler, Kenneth, author.
Title: A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0) / Dan Shoemaker, Anne Kohnke, Ken Sigler.
Description: Boca Raton, FL : CRC Press, [2016] | Series: Internal audit and it audit ; 3 | Includes bibliographical references and index.
Identifiers: LCCN 2016000233 | ISBN 9781498739962 (alk. paper)
Subjects: LCSH: Computer security. | Computer security--United States. | Computer networks--Security measures. | Computer crimes--Prevention.
Classification: LCC QA76.9.A25 S493 2016 | DDC 005.8--dc23
LC record available at http://lccn.loc.gov/2016000233

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword

If you are interested in the field of cybersecurity, it is my personal opinion that you should read this book. Knowing the breadth and depth of the cybersecurity profession is essential in matching your individual talents and desires to efforts that identify threats, defend our national security, protect our national economy, and preserve our way of life.

There are plenty of examples of miscues in our cybersecurity world. Thwarting, guarding, and being a champion requires extensive education, training, and experience. This book, *inter alia*, focuses on each aspect of the cybersecurity profession to provide insight to every reader. It provides an excellent discussion and overview of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Framework (v2.0).

There isn't a version 2.0 without a version 1.0. Stepping back in history just a moment, the Cybersecurity Framework (v1.0), developed under the auspices of the National Institute of Standards and Technology (NIST), was born largely due to the increase in cybersecurity incidents, the need for education and funding, and Congress asking the question "how many cybersecurity professionals do we have in the government?" Until defining what cybersecurity work is, answering with any precision of who was doing cybersecurity work was nigh to impossible! Version 1.0 provided that definition and was the result of a successful concerted effort with (primarily) the government to define the cybersecurity roles.

Even before the Cybersecurity Framework (v1.0) was on the street in 2012 the need to expand the universe of information beyond the government to include industry and academia had become obvious. All aspects of the triumvirate of industry, academia, and government were concerned with the constant and expanding cyber threat to our nation's defense and economic well-being. You name a sector of our society and the cyber threats were (and remain) at the forefront of CEO, CFO, stockholder, and congressional et al. concerns.

To make the NICE Cybersecurity Framework effort truly reflect the national picture, the Framework (v2.0) effort was born. Using Framework (v1.0) as a baseline, planning started in early 2013. By late summer the focus groups started. In the interest of achieving the greatest breadth and depth, the goal for each focus group was to have equal representation from industry, academia, and government

(all levels of government). No organization would be represented more than once, and if for some reason an organization attended more than one focus group, the same person did not attend more than once. These focus groups diligently hammered on each Cybersecurity Framework category and specialty area for quality definitions, completeness/sufficiency of substance, and application to their respective disciplines and organizations. Consensus within each focus group was needed and achieved, and the results summarized.

Knowing how absolutely critical the definitions of cybersecurity categories and specialty areas are to every part of our national structure, once the "strawman" Cybersecurity Framework (v2.0) was available, the focus group approach was repeated as a quality review—new focus groups concentrating on what the prior focus groups had developed. The Cybersecurity Framework (v2.0) provides cybersecurity definitions, as well as knowledge, skills, and abilities that are vital to our nation's success now and in the future. The significance of including the most accurate and comprehensive data was paramount.

In late spring of 2014 the Cybersecurity Framework (v2.0) was completed. The cybersecurity profession is not yet stable. It continues to evolve. However, the lessons in this book will be the basis for whatever transpires and their importance cannot be overstated. Successfully thwarting the evolving threats, the defense of our national security, the protection of our national economy, and the preservation of our way of life depend on you!

Roy Burgess
Former Lead, NICE Cybersecurity WorkforceTraining and Professional Development
Department of Homeland Security

Preface

This book presents a comprehensive discussion of the National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and National Initiative for Cybersecurity Education (NICE) Framework (v2.0). The NICE framework was created by the U.S. NIST to delineate the complete spectrum of task, knowledge, skill, and ability (KSA) requirements for the cybersecurity workforce, as well as to provide a common taxonomy and lexicon by which to classify and categorize cybersecurity workers.

The framework is a major national initiative, which is very ambitious in scope. Its elements are intended to communicate a global picture of cybersecurity work, as well as to provide a detailed explication of "how" the relevant aspects of the seven general competency areas of the profession interact in order to ensure suitable performance of that work. The NICE framework can be easily joined with the purpose and intent of another important NIST model, which is the cybersecurity framework (CSF). In that respect, the tasks specified in the NICE model can be factored into the functions specified in the cybersecurity framework. Or in even more practical terms, the NICE model will specify what the particular specialty area of the workforce should be doing in order to ensure that the CSF's identification, protection, defense, response, or recovery functions are being carried out properly. The association between these two highly influential models will be maintained in the discussion of each of the knowledge areas.

The attendant KSA specifications for that specialty area offer elaboration and clarification of the requisite competencies and the actions to be taken to perform the task. Using these two large-scale frameworks it is possible to construct a detailed picture of the proper organization and conduct of a strategic infrastructure security operation. And in that respect, these two frameworks provide the detailed explication of the discipline of cybersecurity as a whole. Thus, as a combination these two models can serve as an explicit definition of the field of cybersecurity.

Why the NICE Initiative Is So Important

The massive scope of the NICE endeavor and the time and effort expended in developing the framework makes NICE the first complete and fully sanctioned definition of the field of cybersecurity. Up to this point, any delineation of this emerging

field has been shaped by the background, interests, and biases of the people who are providing the description and therefore cannot be considered authoritative. NICE embodies a carefully researched, all-encompassing presentation of every one of the elements of the profession of cybersecurity. And so, in effect, a full understanding of NICE represents complete mastery of the body of knowledge (BOK) of the field.

The NICE framework is generally considered to be authoritative because it was prepared through a 3-year, highly rigorous process spearheaded by NIST. As a result, NICE "officially" specifies the contents of the field. The ability to put the general shape of the cybersecurity profession into perspective as well as to understand all of its elements is a critical requirement for any professional situation or instructional function that purports to be based on the elements of cybersecurity.

The level of detail provided for each of the specialty areas in NICE makes it possible to structure either a single organizational activity or an entire educational experience based on concrete and officially sanctioned descriptions of KSA competencies. Thus, using the framework managers and educators can be brought to a common understanding of what is required to suitably perform cybersecurity work.

Justification for the NICE Approach

The framework is by necessity vast in concept and therefore the top-level approach that we use in this book is crosscutting. Our aim is to convey the complete contents of the field. In effect, what we are presenting here is an overview explication of the framework, its concepts, the underlying relationships between the areas, and the general content of those areas. In essence, the purpose of the book would be to explain *what* is in the framework and how it relates to the requisite functions in the CSF.

Practically, the textbook can serve as a roadmap of sorts. Because of the scope of the framework, the understanding we are conveying is aimed at Bloom's level two "comprehension" of the total concept and elements of the NICE model. The text serves as the necessary guide to the content areas. The reader can then drill down to whatever level of specificity they desire using other, more focused material. The general goal is to provide comprehensive support for a strategic view of the profession.

In essence, this book will provide a comprehensive roadmap that will allow a person to understand the application and uses of the NICE content. This also holds true for applications of this book in education and training situations. NICE is authoritative, both in job definition and also in terms of defining the work to be done for a particular organizational use. The job-task definition aspect is important because the framework supports the Presidential Job-Driven Training Initiative, which is a recent Presidential Directive (June, 2014).

The NICE initiative has been specifically aligned with the Presidential Job-Driven Training Initiative. As such, NICE will form the core of the comprehensive

federal effort to increase the number of workers who complete high-quality cyber training programs and attain skills that are in high demand in the federal and national workforce.

One of the advantages of the NICE approach is that it does not define security as a monolithic field or a single profession. Instead, it provides the complete assortment of required task and KSA competencies for a range of 32 specialty areas and functions. That set can then be tailored and adapted to any relevant situation. Thus, for readers, this book will have a comprehensive description of how to do it right.

In industry, the people who would benefit from this knowledge range from managers through all types of technical workers and specialists. As such, depending on the tailoring it would be possible to make the case that in order to be considered to be performing a function properly that activity should embody some, or all, aspects of the NICE KSAs. The NICE framework applies to anybody who wishes to demonstrate authoritative and standard cybersecurity knowledge and competencies appropriate to their personal, career, or professional area of interest. That would apply from individual tasks all the way up to the strategic planning initiatives that will be required as the profession evolves.

In terms of practical personnel development, the ability to demonstrate standard KSA requirements can be used to validate adequate mastery of the necessary skills for a given workforce role. As a result, the competencies defined for each functional role in the framework ought to eventually become the yardstick to judge whether an employee has the necessary KSAs to do the work.

Unlike any other presently existing books, the value of this book is that it is based around well-accepted standard recommendations rather than presumed expertise. Some of the recommendations presented in this book are brand new; however, the core of the NICE framework has been established and vetted over an almost 4-year period, and its correctness has never been questioned. Therefore, the content of this book would not be a matter of opinion or even a recent fad. It would represent the current best knowledge about the practices to assure an authoritative definition of cybersecurity work. In that respect it is based on a recognized and formally promulgated BOK, which underlies a national level initiative to standardize the profession and which is tied directly to career paths.

That is the key message here. This book is based on a brand-new and unique national level initiative. This is the only book that aligns with and explains the requirements of a national level initiative to standardize the study of information security. Moreover, the knowledge elements contained in the book represent the first fully validated and authoritative BOK in cybersecurity. This book directly relates the requisite security knowledge to specific career tracks and job titles. In addition, it relates this knowledge to the functional requirements of the CSF. Its role-based competencies can be tailored to every level of enterprise and it is likely that commercial certificate authorities will decide to demonstrate that they meet the requirements of the NICE framework. If that is the case, this book will support study to obtain professional level certifications.

Intended Audience

This book is designed to give the reader a comprehensive understanding of cybersecurity work in all of its manifestations. Its recommendations are relevant for a range of professional roles and functions within that profession. The recommended practices for these roles and functions can subsequently be tailored to any relevant application within professional information technology (IT) practice. Thus, the audience could include anyone who wants to gain an understanding of all the KSAs that are appropriate for a particular professional role or academic interest.

The audience in the business world can include everyone from managers and technical workers to specialists such as auditors, testers, and general IT staff. From an organizational standpoint, this book was designed to align with several IT security models, such as the ISO 27000 series and also NIST SP 800-53(4). From the standpoint of higher education, the audience might include students who want to learn how to effectively perform a cybersecurity role and instructors who want to prepare their students for the pragmatic world of cybersecurity work. The tasks and KSA specifications embodied in NICE might also be considered sufficient to satisfy the requirements of commercial certifications for IT security assurance and certification schemes like DoD 8570.

Organization of the Text

The NICE model represents the accepted definition of cybersecurity work. The aim of the NICE workforce model is to provide a comprehensive and detailed set of recommendations about best practice for seven areas of cybersecurity work. The text is organized to help the reader understand how each of these knowledge areas can produce a practical, working cybersecurity solution.

NICE is ideally suited to educators because of its purpose. Unlike other umbrella frameworks, the NICE model was specifically designed to provide detailed task and knowledge requirements for the profession as a whole. Thus, the NICE model is a single authoritative description of the BOK as it applies to every type of professional cybersecurity work.

A comprehensive specification of the requirements for the multitude of roles contained in the model will help an organization tailor best practice to meet its real-world needs. Using a tailoring approach, the organization can create a practical, everyday set of work instructions that are customized to fit its exact needs. More important, the organization can adjust those practices as the situation evolves to ensure a continuing correct response.

This book is divided into two parts. The first part of this book comprises three chapters that give the reader a comprehensive understanding of the structure and intent of how the NICE model, its various elements, and their detailed contents. Chapter 1 introduces the concept of standard definitions of roles within the

32 specialty areas of the framework. This introductory understanding is necessary because the NICE model is descriptive not prescriptive. Therefore, the purposes and intents of the specialty areas have to be fully understood in order to be properly applied. Chapter 2 introduces the explicit tasks and KSAs within each of the specialty areas. Chapter 3 introduces the CSF functions, which define and focus the actual security work within each specialty area.

The second major part of this book, Chapters 4 through 10, introduces each knowledge area individually. Each knowledge area is specifically designed to enable the security goals of a particular aspect of cybersecurity work. The detailed content of the model is presented here. Two of the knowledge areas are combined in Chapter 8. These are the intelligence tradecraft–related parts of the model. The overall objective of this book is to help the reader build a comprehensive understanding of how to organize and execute a cybersecurity workforce definition using standard best practice. To reinforce the reader's understanding of the text and to ensure a successful learning experience, we have provided the following features:

- *Chapter Summary: A bulleted list provides a brief but complete summary of the chapter.*
- *Key Terms: A list of all new terms and their definitions is included in each chapter.*

Acknowledgments

We sincerely thank Dan Swanson who graciously and quickly approved our proposal idea and provided great support throughout the project. We also thank Rich O'Hanley for his support and all of the talented folks at Taylor & Francis who worked very hard to produce what you see.

A book like this expresses the work experiences and education of not only the authors but the team of people who authored the NICE Framework. We are indebted to the team of people who recognized the lack of consistency of how cybersecurity work is defined and the absence of a common language to understand cybersecurity work. It is our hope that our contribution will aid in the NICE Cybersecurity Framework becoming the body of knowledge for the cybersecurity field.

CYBERSECURITY

1

Defining Competencies for the Cybersecurity Workforce and Two Frameworks

Chapter 1

Introduction: Defining the Cybersecurity Workforce

Chapter Objectives

At the conclusion of this chapter, the reader will understand:

- Why security in cyberspace is important
- The issues that have to be overcome in order to ensure cybersecurity
- Two common sense factors that make cybersecurity different
- The general structure and intent of the National Initiative for Cybersecurity Education (NICE) framework
- The general application and justification for the NICE framework
- The elements of the NICE framework

Cybersecurity: Failure Is Not an Option

Computerized systems and the information they process are so tightly bound within the fabric of our society that their reliability and the confidentiality, integrity, and availability of the information that they process must be totally trustworthy in order to enable the fundamental structures of our society.

For instance, one only has to imagine the impact on its customers, if the information that was kept in a bank's databases was corrupted or lost. Or imagine what would happen if national defense information was leaked to our adversaries. Yet the average bank executive or governmental manager has great difficulty appreciating the true value of the systems and information that they manage.

The problem lies in deciding what security is worth to an organization. In a profit-driven world, it is hard for the leaders in the public and private sectors to justify the tangible expense of protecting virtual assets like computers and networks, and their contents. As a result, even though the constituent elements of cyberspace have real value and can directly impact people's lives, it is hard for the people who are putatively responsible for the protection of those contents to understand how the ways that the theft or destruction of a computer or its information might affect them personally.

Equally as important, it is exceedingly difficult and very costly for any organization to ensure reliable and systematic protection for an asset that is as dynamic and abstract as its information technology (IT) systems and information.

The problem lies in the fact that the knowledge that is required to assure reliable and consistent protection of cyber assets changes as rapidly as the technology evolves. As a result, most people view the practices involved in ensuring cybersecurity as an opaque set of activities and requirements that nobody outside the elected few can truly understand or apply.

As a consequence, America's electronic infrastructure is riddled with vulnerabilities that have underwritten an outrageous number of criminal and national security exploits over the past decade. For instance, according to the nonprofit Privacy Rights Clearinghouse we have lost over one *billion* records in the past 10 years. And you should keep in mind that those losses only comprise the outcome of breaches that were *reported*. Since most companies do not like to publicize their security failures that number could be, and probably is, much higher.

The running average of 100 million records reported lost per year has been subject to some variation over time and the source of breach has changed in logical ways. But, the number of reported incidents rose annually from 108 in 2005 to 607 in 2013. And you should still keep in mind that these are only the ones that were reported. So it would be unrealistic to conclude that we have been getting better at protecting information.

Six Blind Men and an Elephant

The problem stems from the fact that the field of cybersecurity suffers from the "Six Blind Men and the Elephant" syndrome. In that old story six blind men are asked to describe an elephant based on what they are touching. So to one, it's a snake, another, a wall, and to another a tree, and so on. In the end, "Though each was partly in the right, all were entirely wrong." (See Figure 1.1.)

We have the same problem with knowing what to do to protect our system and information assets. There are established elements of the field that know how to secure the part of the elephant that they touch. But until we are able to amalgamate that knowledge into a single coordinated solution we cannot realistically say we are protected.

It should be obvious that highly complex problems cannot be solved piecemeal. Effective solutions can only be based on whole system approaches. Or in simple

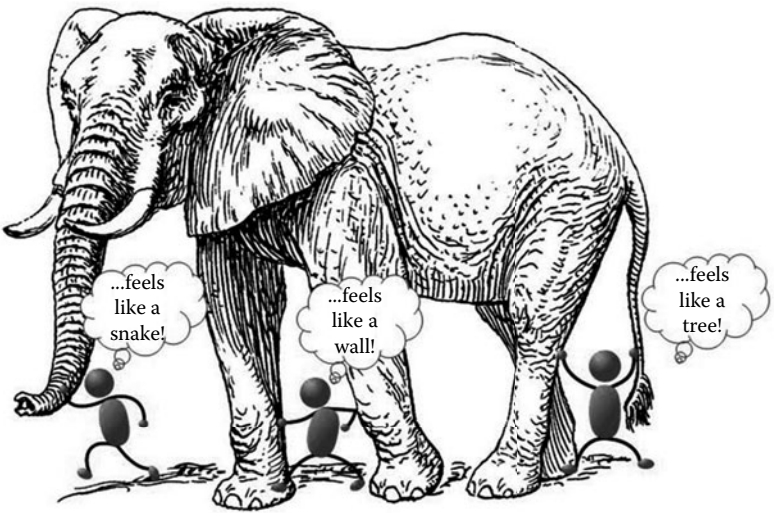

Figure 1.1 Blind Men and the Elephant syndrome.

terms, "You are not secure if you are not completely secure." Those solutions have to encompass the entire body of knowledge and be taught as a coherent entity, within a disciplinary framework. Needs may vary in their particulars within the overall scope of the problem. But it is important to keep in mind that the elephant is a lot bigger than its individual parts. So you have to understand the entire beast in order to master it.

Cybersecurity: An Emerging Field

The issues associated with cybersecurity can be dated to the advent of the commercial Internet in the mid-1990s. Accordingly, the entire profession has a less than 20-year life span. In that time, cybercrime, cyberespionage, and even cyberwarfare have become visions with real consequences. Consequently, until there is a single commonly accepted definition of the field and the profession it is unrealistic to assume that our way of life is adequately protected.

Yet, even with its newfound national prominence, there is still a lot of disagreement about what legitimately constitutes the right set of actions to prevent harmful or adversarial actions. That disagreement was captured in a 2013 report sponsored by the National Academy of the Sciences (Bishop and Burley, 2013).

The report asserts that cybersecurity is at best an ill-defined field, which is subject to a range of interpretation by numerous special interest groups. Since there has been heretofore no clear definition of the field, the profession and the actual protection of computers and information tend to be characterized by a long track record of hit-and-miss failures (Figure 1.2).

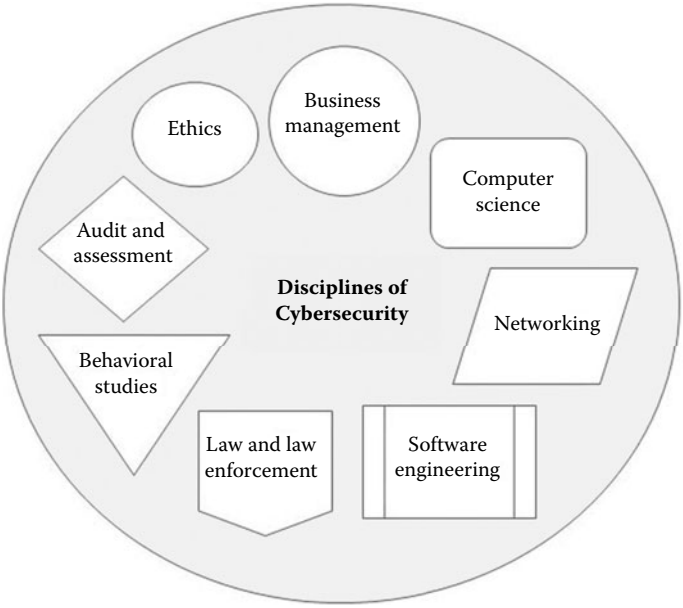

Figure 1.2 The variety of disciplines involved in cybersecurity.

The confusion about what constitutes the proper elements of the field originates in the fact that the profession of cybersecurity could potentially comprise concepts from a number of disciplines. Some content from all of these disciplines might reasonably fall within legitimate boundaries, which includes such diverse areas as the following:

- Business management, which contributes concepts like security policy and procedure, continuity planning, personnel management, and contract and regulatory compliance to the cause.
- The traditional technical studies of computer security, such as computer science, contribute knowledge about ways to safeguard the processing of information in its electronic form.
- Likewise, knowledge from the field of networking adds essential recommendations about how to safeguard the electronic transmission and storage of information.
- Software engineering adds the necessary system and software assurance considerations like testing and reviews, configuration management, and life cycle process management.
- Law and law enforcement contribute important ideas about such topics as intellectual property rights and copyright protection, privacy legislation, cyber law and cyber litigation, and the investigation and prosecution of computer crimes.

- Behavioral studies address essential human factors like discipline, motivation, training, and certification of knowledge.
- Even the field of ethics, with its consideration of the personal and societal implications of information use and information protection, as well as codes of conduct contributes something to the discussion.

All of these areas could potentially bring something to the overall aim of information protection. As such, it would seem logical to incorporate the principles and methods from each area into the total body of best practice for cybersecurity. Nonetheless, at this point there is still discussion about where the line ought to be drawn or where the focus within those boundaries ought to be, that is, where two simple common sense principles come into play.

Two Common Sense Factors That Make Cybersecurity Different

The factors that make securing systems and their information different from any other form of security endeavor can be summed up by two common sense factors. The first factor is the availability paradox; that is, systems and information have to be optimally available in order to be of any value to their user community. Yet the very requirement for maximum availability makes it difficult to ensure the confidentiality and integrity of that information. In essence, one critical condition, availability, trade off against the other two essential conditions, confidentiality and integrity.

The second factor is more overarching. It is called the "complete protection" principle. In essence, under this rule the system is not secure if any part of it can be exploited. The rule that emerges from the "complete protection" principle is that if a cyber-related situation is to be considered adequately secured, every potential instance of risk and exposure within that system has to be mitigated at all times by a formally defined and maintained protection mechanism.

The real-world condition that makes complete protection hard to sustain is the fact that the availability paradox demands that the information be easily available. In simple terms all protected information has to be obtainable by the user, at the time that they want to use it. This implies that all system and information assets have to be easily accessible while being fully protected.

This is a condition that is very difficult to achieve because important information might exist in three different forms at the same time. In essence, a critical piece of information might exist in a physical form, on paper records for instance, while it is also present in electronic form on servers or even in portable devices like a tablet computer. And even, to stretch the point, that same information might be in the head of an individual.

The problem for security is that every one of those places has to be identified and properly protected in order to ensure that a particular system or information

asset of value is actually secure. Otherwise, a compromise of an instance of the item in one location will in essence compromise all other instances of the same item in all other places.

The only way to make certain that a compromise does not occur is to identify all instances of the information and then put technical and/or management controls in place to ensure trusted access. Nonetheless, in order for those controls to be effective, they have to be coordinated. That coordination is normally supplied through a single unified management process. The figurative term for that all-inclusive management process is "information governance."

In its simplest form, information governance ensures that the organization deploys and controls all of its cybersecurity-related functions through a single coordinated means. That specific approach ensures the deployment and subsequent sustainment of a set of mutually supporting controls or countermeasures.

The purpose of a well-defined and formally implemented information governance function is to integrate the requisite set of countermeasures into a coherent operational activity that will theoretically address every known area of potential exploitation. It should be obvious from this requirement that the information governance function has to be adapted, or customized, to meet the needs of each specific situation. Moreover, within that customization process, the designer will have to take into consideration all relevant protection requirements as well as provide the most single effective means of assuring the necessary level of trust.

Instilling Order in a Virtual World

The problem with cybersecurity is that the contents and activities that are done in the virtual world are nothing more than a proxy for human actions in the real world. The value of a piece of information might be derived from the importance of the idea, or the criticality of the decision, or it can represent simple things like doing your taxes or keeping track of your bank balance. Nonetheless, the fact remains that until the tangible outcome and value of that information or programmed action is known and analyzed for inherent risk, it is hard to talk about the concrete mechanisms for protecting it.

So the first problem for cybersecurity professionals is to simply identify and then prioritize those things that are necessary or useful to satisfy the organizational mission. And in conjunction with that they also need to sort out the things that are not. Given the fact that most organizations are awash in digital information and computerized functionality, this is not like finding the proverbial needle in a haystack. It is more like trying to sort out the right needles from a much larger pile of needles. So the first step in any cybersecurity process is to simply get it organized.

That assignment would be relatively easy if you could actually see the information. But since cyber-information is both virtual and easily changed it is essential that the people responsible for assuring trust follow a disciplined and well-defined process. That process has to consistently assure that all organizational systems, and information, of any potential value are identified, assessed, and prioritized. If that identification, assessment, and prioritization activity is comprehensive and accurate, a properly organized cybersecurity process can be created.

Any system or information asset is a potential target for control based on its intrinsic value to the organization. Systems incorporate all of the hardware and system assets, applications, facilities, and personnel that store and process it. Nonetheless, with the exception of hardware, personnel, and facilities, all of these assets are intangible. So, they are not easily accounted for.

It should be clear that in order to have proper security it is important to specifically designate the actual target of control. However in most companies, systems extend everywhere, in some cases globally. And information flows back and forth across organizational boundaries, both virtually and physically.

Worse, the practical business processes of a complex organization can be very diverse, ranging from high finance to shipping and receiving. Moreover, those processes are usually dispersed to a wide range of locations. The need to ensure information in highly diverse and widely dispersed settings gets us back to the problem of intangibility.

It is easy to account for the flow of parts from an inventory or even the physical flow of dollar bills from a teller's till, because these are tangible items that can be seen and accounted for. Actions can be taken based on the ability of the person performing the transaction to actually see and control what has taken place.

Neither systems nor the information they process can be controlled that way, because even though information flows to and from a single point, usually a server, that server can be accessed from an infinite number of locations, thanks to the Internet. Moreover, that access is in the virtual world.

For instance, the whole point of a network is to provide remote access for users. The problem with controlling that access lies in determining who to trust. The responsibility of the cybersecurity process is to ensure that determination is correct. Effective control of access requires the ability to ensure that access is only granted to trusted people.

That implies the need for a formal process that will identify the right individuals and assign the appropriate access privileges. Then, the formal regulation of their access can entail the automated controls and managerial factors, which are integrated into a tangible framework. That framework is operationalized through explicit managerial control objectives and rules, which in their documented form represent the prescribed approach that the organization will use for ensuring trust. The creation of a comprehensive well-coordinated organization-wide set of rules and procedures is the function and purpose of the information governance process.

Combining Effort with Intent in Order to Get a Complete Solution

It goes without saying that, in order for a defense to be effective, all of the requisite countermeasures have to be in place and properly synchronized. This might seem like a self-evident statement, but the fact is that the typical cybersecurity solution will most likely only embody those measures that fall within the specific area of interest and expertise of the people responsible for the approach. Figure 1.3 shows systems, physical space, and stakeholders that together make up a complete solution.

Accordingly, the approach itself is likely to include only those countermeasures that the designers feel are necessary to secure their particular area of responsibility. For instance, if the security of systems and information is seen as a responsibility of the network security people, they are likely to install a firewall and electronic intrusion detection system (IDS). But electronic countermeasures alone will not protect a company from an authorized insider. So a company that relies only on a firewall and IDS solution would be vulnerable to insider theft.

Moreover, a defense that only reflects the focus and interests of a single field will almost certainly have exploitable holes in it. This can be a fatal flaw for any business because any competent attacker will simply scout around for the holes that they know must exist. That is why it is important to involve all of the fields necessary for assurance of that security in the design process, including electronic, personnel, and physical elements. Obviously, if a number of disparate fields are involved it is important to also ensure that the right disciplines are engaged in the overall process by which cybersecurity is both implemented and overseen.

Full involvement of all stakeholders is a very important consideration because of the requirement that no gaps can exist in the defense. For instance, IT installs

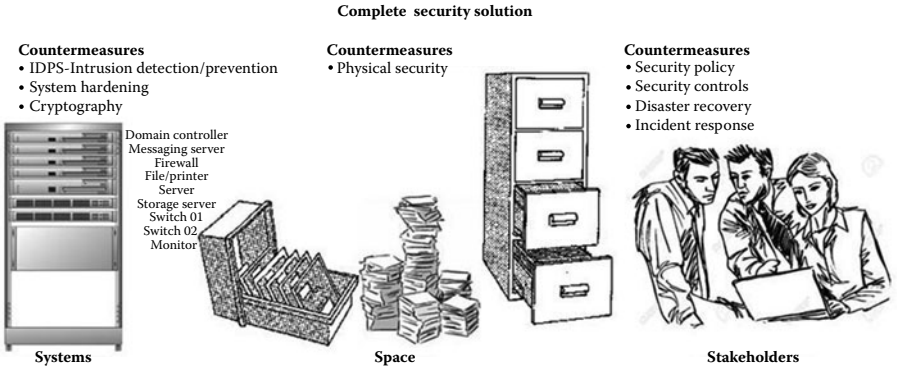

Figure 1.3 Systems, physical space, and stakeholders that together make up a complete solution.

technical countermeasures but it rarely has the responsibility to deploy accompanying physical security controls. Further, while the physical security team might deploy a complete set of physical protection measures, those are rarely coordinated to work in conjunction with the electronic measures utilized by IT to control external user access to their systems.

In fact, in most organizations physical and electronic security involves two entirely separate and independent areas of the company. As a result, gaps in the defense are likely to be created simply because the electronic and physical access control measures are not properly deployed, overseen, and maintained.

Ensuring effective alignment between the countermeasures that have been developed by the various security specialties might be difficult. But, to make matters even worse, most systems and instances of information exist simultaneously in more than one form. For example, customer sales information can be recorded electronically, but the same information can also be written down in a sales book, or just remembered. Therefore, the only way to ensure adequate security is to identify both the critical items of information, as well as all of the places where that information might conceivably be processed and kept.

A reasonably accurate inventory of the important information that the organization has and where it resides is important, because that inventory will allow security designers to establish the right set of procedural, environmental, technical, and human controls to secure its contents. Besides targeting the right information items, these controls also need to ensure that the protection applies to all instances of the information item wherever it is kept across the entire organization.

Finally, any workable solution has to be practical, that is, the overall array of protection measures has to operate within a well-defined and economically feasible management infrastructure. This requirement embodies Saltzer and Schroeder's "Principle Number One, Economy of Mechanism" (Saltzer and Schroeder, 1974). That infrastructure should reflect the assurance needs of the business as well as its business requirements. And the controls themselves must provably address the known threats they are designed to target.

Finally the security scheme itself should be assured to be trustworthy over time. The latter condition just ensures that the protection evolves as the asset base and the threat environment evolve. This is an absolutely necessary consideration because the outrageous evolution of the technology is one of the primary causes of disjointed and therefore easily exploitable security approaches.

Cybersecurity: Finding the Right Set of Activities

As we have seen by example here, cybersecurity, as a basic condition and requirement, is far too broad a concept to be a simple technological concern. Therefore, the cybersecurity process has to be founded on, and sustained by, a well-defined and formally structured organization-wide governance process. The goal of that process

is to develop and integrate every requisite technology and management control into a global and sustainable organization-wide system, which is able to meet the assurance needs of each specific threat.

The role of cybersecurity is to ensure that all of the system and information resources necessary to underwrite a particular business strategy are kept robustly, confidential, correct, and available. The process of providing that assurance has to fit within the day-to-day business model and it should always add some value to the enterprise's overall purposes.

One of the common complaints about the everyday actions that are necessary to ensure a safe environment is that those activities slow down, or otherwise adversely impact the business process. Moreover, they are additional overhead so they are seen as costly. Therefore, one of the most important conditions for the development of an effective, comprehensive cybersecurity solution is that the actions involved in ensuring security cannot get in the way of effective and efficient business operation. That requirement is the reason why "Economy of Mechanism" is Saltzer and Schroeder's Principle Number One (Saltzer and Schroeder, 1974).

Thus, the aim of a formal cybersecurity process should always be to maintain an optimum and secure relationship between each of the company's business processes and their respective computerized resources. In that respect, the cybersecurity process needs to create and maintain an optimum set of technical and procedural controls to ensure the protection of all distinct systems and information utilized by each business process.

In practice, cybersecurity develops the specific policies, organizational structures, practices, and procedures needed to achieve effective assurance. Operationally, that involves the definition of explicit procedural and technical controls for any given requirement. These controls should ensure the effective management and operation of all cybersecurity functions.

The comprehensive organizational control structure, which is the operational incarnation of this process, must always be appropriate to the security requirements of the entity being controlled. It must also be consistently executed.

Thus, the control structure itself embodies a carefully designed and explicitly maintained set of electronic and managerial control behaviors, the outcomes of which can be observed and documented. The controls themselves are rarely standalone. They are normally integrated along with a range of other types of control to produce a verifiable state of sustainable assurance.

In order to make sustainment practicable, the coordination and management of the cybersecurity function itself should be located at the policy development and enforcement level of the organization. That is normally called the "C" level.

Anchoring the process at that level is necessary because the cybersecurity function itself must always be planned and administered from the organizational level where requirements can be enforced. That level of managerial commitment is essential because the executive-level decision makers are the only people who have

the legitimate authority to create and enforce policies and procedures that might be unpopular across the entire organization.

That requirement is reinforced by the fact that cybersecurity is overhead to organization. Therefore, the people at the top have to be actively involved in sponsoring and directly engaged in the development of the strategic plan to ensure the requisite degree of protection for the business. The problem is that most top executives frequently see cybersecurity as a technical exercise. As a result, even though a big enough compromise can literally ruin a company, top-level managers do not think that cybersecurity is their problem. Consequently, they shift that responsibility down to the managers of the functional areas.

This is a mistake because nobody at the managerial level in the next level down has the authority to maintain a given process outside of their own area. And as a consequence, the assurance measures that might be implemented by each given manager in their particular area are likely to be a patchwork of actions. And the piecemeal nature of those activities will create gaps that will be exploitable.

Changing Times, Changing Players: The Stakes Get Higher

In day-to-day practice, the number of defenses that are weak or exploitable have been increasing over the past decade across the spectrum of government, business, and academe (PRC, 2014), because the number and type of attackers is growing in size and sophistication. In the 1990s, a typical attack was something like a criminal trespass, or Web site defacement. The victims tended to be the usual list of suspects, such as government institutions, and attackers themselves were inclined to be counterculture types who worked alone and on the fringes (Schmalleger and Pittaro, 2009).

That situation has changed, as the Internet has become the medium of choice for commerce. Now instead of being inspired by a desire to prove their art, attackers are motivated by financial gain and political ends. As a consequence, the old stereotypical image of the kid living on candy while doing 72-hour hacks out of his mom's basement has been replaced by a much darker and more complex persona, one who is well organized and much more focused on making trouble.

For instance, there are organized groups who perpetrate large-scale raids on financial institutions for the purpose of theft. In fact, the opportunities for financial gain from cybercrime are so great now, that established organized crime syndicates have taken to the business of electronic crime with the same zeal and enthusiasm as they did in the past with traditional physical crimes.

However, this new criminal business does not involve guns and strong-arm tactics. Instead it involves all of the potential ways that information can be obtained and exploited, ranging from sophisticated hacking to dumpster diving.

That range of new exploits raises one final concept, that is, the legal principle of "due care," which is sometimes called "due diligence." Due care is nothing more than the ability to prove that all reasonable precautions were taken to prevent harm resulting from an attack on something that you are legally responsible for. The problem is that, up to this point there has never been a standard definition of what constitutes due diligence in the information protection realm. Now that various models exist as it is possible to judge whether a company has been legally negligent in the way it handles an individual's personal information, that is, where the emerging numbers of best practice standards come into the discussion.

Definitive Step to Ensure Best Practice in Cybersecurity

In simple, operational terms, the cybersecurity process involves nothing more than deploying and then ensuring a coherent set of best practices to protect all assets of value to a particular company. The problem lies in the term "best practice." As we saw with the elephant, everybody has their own definition of what constitutes best practice. So, the actions that one group might view as appropriate to secure an asset may not be seen quite as appropriate to another group.

Therefore, it is essential to adopt a complete and commonly accepted framework of correct practice as a point of reference to guide any actions that an organization might take to protect its assets in the real world. The ideal would be to have that framework authorized and endorsed by a universally recognized and legitimate third party.

In the case of cybersecurity, the best practice framework ought to encompass all of the legitimate actions necessary to ensure a reasonable state of reliable long-term security. Then, with respect to evaluating whether due care has been taken, it can be assumed that, if all of these practices are executed properly then the organization has met its legal and ethical obligations for information protection.

Many other professions, such as the law or medicine, have a commonly agreed on definition of what it takes to meet the minimum standard of due care. Those help set the boundaries of ethical practice as well as guide the correctness of actions within those boundaries. Up to this point however, the problem for cybersecurity professionals is that generally accepted framework did not exist.

So the question became, "what criteria should a model for best practice in IA meet"? Ideally, a model for good cybersecurity practice would be universal in its application. Its correctness would be commonly accepted within the practitioner community. The model's recommendations would embody all of the currently understood correct actions for ensuring the confidentiality, integrity, availability, authentication, and nonrepudiation of information. Moreover, those recommendations would be expressed in a form that would allow a competent practitioner to tailor out a practical and economically feasible system that would protect all of the information of value under their care.

The lack of an acceptable model of the field has been an obvious roadblock to success for a very long time. As a result, the National Institute of Standards and Technology (NIST), which is the standards body for the federal government, was tasked to create a conceptual model that could serve as the single definition of the specialty areas, roles, and job tasks of the field.

During the period 2011 to 2014, the project was authorized and executed as the NICE Initiative. Besides NIST's involvement, the project was staffed and jointly executed by personnel from the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM).

NICE workforce framework defines the complete set of roles that might reasonably be necessary to identify and mitigate all emerging threats in cyberspace. As a whole, the responsibility of those roles is to ensure the most economical and practical level of trust in the integrity and security of information and communication technology (ICT) assets. In essence, the NICE framework defines the field of "cybersecurity."

The structure and content of the NICE framework is generally considered to be the single definition of the field, which had previously been lacking. In that respect, NICE represents the most authoritative picture possible of the whole elephant and therefore it should be considered to be currently definitive. Moreover, due to its role as the definition of the elements of the field a thorough understanding of those elements and the requisite knowledge, skills, and abilities (KSAs) involved in executing them is an essential for any person who desires an in-depth understanding of the field. The aim of this book is to provide that understanding.

National Initiative for Cybersecurity Education Initiative

Cybersecurity is an emerging profession. Fifteen years ago, the notion of a workforce entirely dedicated to the protection of ICT assets would be unheard of. Nonetheless now, especially with the critical role that systems and computerized information plays in every aspect of our lives, a formally defined profession that is dedicated to developing effective ways to assure trust in the confidentiality, integrity, availability, authentication, and nonrepudiation of digital information is right at the forefront of our national priority list.

At present, the actions that we take to ensure cybersecurity are fragmented into a number of camps, all of whom claim that they have the answer. It ought to be obvious from the first sentence that the situation in the second sentence has to be changed if we ever want to be secure. So how do we change it?

The term "holistic" has been used to describe what has to happen in order for the security solution to be complete and correct. But most of the current profession specializes in some vertical aspect of the field. So we will have to reorient our thinking in order to address the problem in its entirety. And we will need a powerful societal force to implement that change.

Fortunately we have society's formal education processes available as a means of effecting change. Throughout time, education has been the mechanism we utilize to shape mass behavior. For that reason, a coordinated program of education can be a powerful public force. And it is education's historical impact on our society that makes it the logical place to start to address the overall problem of cybersecurity.

Nevertheless, there are a number of systemic and cultural challenges that have to be overcome before education can become a practical solution. First, according to a report from the National Academies of Science, cybersecurity is an emerging discipline. Consequently, it is not exactly clear what we ought to teach. Worse, all evidence points to the fact that whatever we should be teaching is cross-cutting. In essence, elements of the discipline of cybersecurity can be taught in places as diverse as engineering, business, medicine, and law.

People who are not academics may not realize the implications of cultural differences in academia. But, the people in those cultures have very different views of what is important and those views tend to be encased in stovepipes. Perhaps more importantly, all of these disciplines compete for students. Thus, their teaching is likely to stress the importance and value of their own content and research agendas to the exclusion of anybody else's.

Cultural differences also raise the question of "to aggregate or not to aggregate." If we leave the teaching of cybersecurity in diverse places on campus, we are not going to get a coherent message, let alone evolve the field into a mature discipline. However, if we pull all of the cybersecurity education into a single place that begs the question of "where should we put it?" since engineers will not play well with law school faculty and vice versa.

It should be obvious that a broad-scale academic strategy has to be based on a comprehensive definition of the field. The federal government has taken the first step in providing that definition with the publication of the NICE National Cybersecurity Workforce Framework (v2.0).

National Cybersecurity Workforce Framework (v2.0)

The DHS's compendium of best practice is titled The National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework (v2.0), and it attempts to satisfy all of those requirements. The NICE framework makes an authoritative, formal statement about what an individual has to know in order to fulfill the requirements of a range of roles in an organization. Figure 1.4 shows the seven general knowledge areas of the NICE Workforce Framework (v2.0).

The framework is a product of the NIST and the Department of Homeland Security National Cyber Security Division (DHS-NCSD). NIST has the advantage of being a federal government entity and so it has the ability to reach across all sectors to assemble a national body of experts. And so given that reach, the experts who worked on NICE were drawn from all of the concerned sectors of our society,

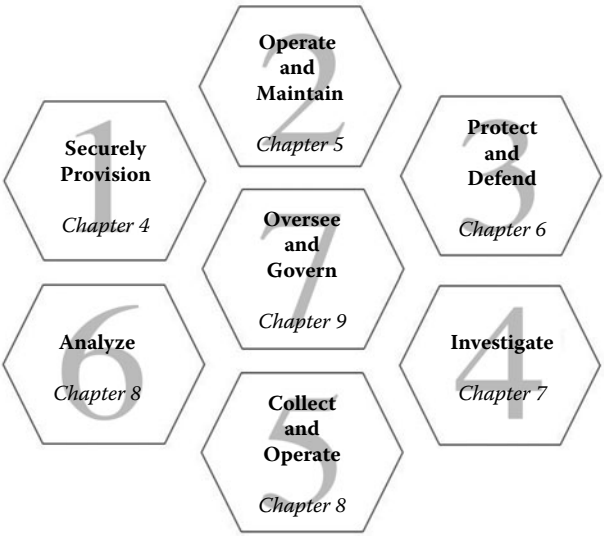

Figure 1.4 The seven general knowledge areas of the NICE Workforce Framework (v2.0).

governmental, business, and academic. That input was then pulled together into a single "national baseline representing the essential knowledge and skills" that all IT security practitioners should possess (NIST, 2014).

The NICE framework is an umbrella framework, in the sense that its intention is to define the complete set of competencies associated with cybersecurity work. However, the NICE model goes a step further in that it also links those competencies to a group of common security roles and a set of functions associated with those roles. That gives individual practitioners a standard set of recommendations about the activities that should be implemented in order to fulfill the requirements of each of those roles.

There have been other attempts to create an inclusive, top-level framework for best practice in cybersecurity. One of the better-known examples of framework models of this type is the International Standards Organization's (ISO) ISO 27000 series of standards. Specifically, ISO 27001/27002 offers a valid model for the definition of an information security management system (ISMS). However, it is not intended as a yardstick to define the common knowledge requirements of a given cybersecurity professional.

There are models that do define personal requirements for practitioners within specific silos of practice. These include the common body of knowledge (CBK) for the Certified Information Systems Security Professional (CISSP) and the Information System Audit and Control Association's (ISACA) Control Objectives for Information and Related Technology (COBIT). Specifically, International Information Systems Security Certification Consortium (ISC2s) CISSP and ISACA's Certified Cybersecurity Manager (CISM) provide a perfectly acceptable

CBK for cybersecurity professionals. However, they are totally different and competing models, in the commercial space, and therefore they cannot be considered to be a commonly accepted basis of the profession.

The aim of the National Cybersecurity Workforce Framework is to "establish the common taxonomy and lexicon to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed" (NIST, 2014). The framework is composed of 7 knowledge areas and 32 distinct specialty areas. These knowledge and specialty areas define the range of activities that legitimately comprise the cybersecurity profession. In that respect, NICE has become the first truly holistic definition of the field.

The framework is intended to be applied in the public, private, and academic sectors. Use of the framework does not require that organizations change organizational or occupational structures. In fact, the framework was developed because requiring such changes would be costly, impractical, ineffective, and inefficient. Thus, the framework can be applied to situations across all types of settings and environments.

As depicted in Figure 1.5, the aim of the NICE model is to standardize the concepts and terms of the profession. These are arrayed into seven areas of common practice:

1. Securely provision
2. Operate and maintain
3. Protect and defend
4. Investigate
5. Collect and operate
6. Analyze
7. Oversee and govern

Those seven areas define the entire range of appropriate activities for the assurance of information. The NICE model also factors the activities in these 14 areas into specific professional practice requirements for 65 standard roles in 32 specialty areas.

Those 65 roles range from "chief information officer (CIO)" to "acquisition specialist." In addition to specifying the acceptable actions for each of these professional roles, the NICE model specifies the appropriate KSA requirements for each specialty role. This degree of explicit direction establishes the NICE model as an ideal conceptual framework to base a practical cybersecurity solution on, for any organization.

In order to aid in implementation, the framework contains a catalog of prototypical specialty areas for each of the seven knowledge areas. The knowledge areas themselves are very broad and deep. In essence, they would be considered a "field" in conventional practice. Examples of that are such fields as forensics (investigate), or software engineering (securely provision). Sample job titles that lie within the 32 specialty areas are provided as examples of common work functions that might fall within each specialty area. They are primarily offered as a means of illustrating and ensuring a practical understanding of the application of the framework in real-world settings.

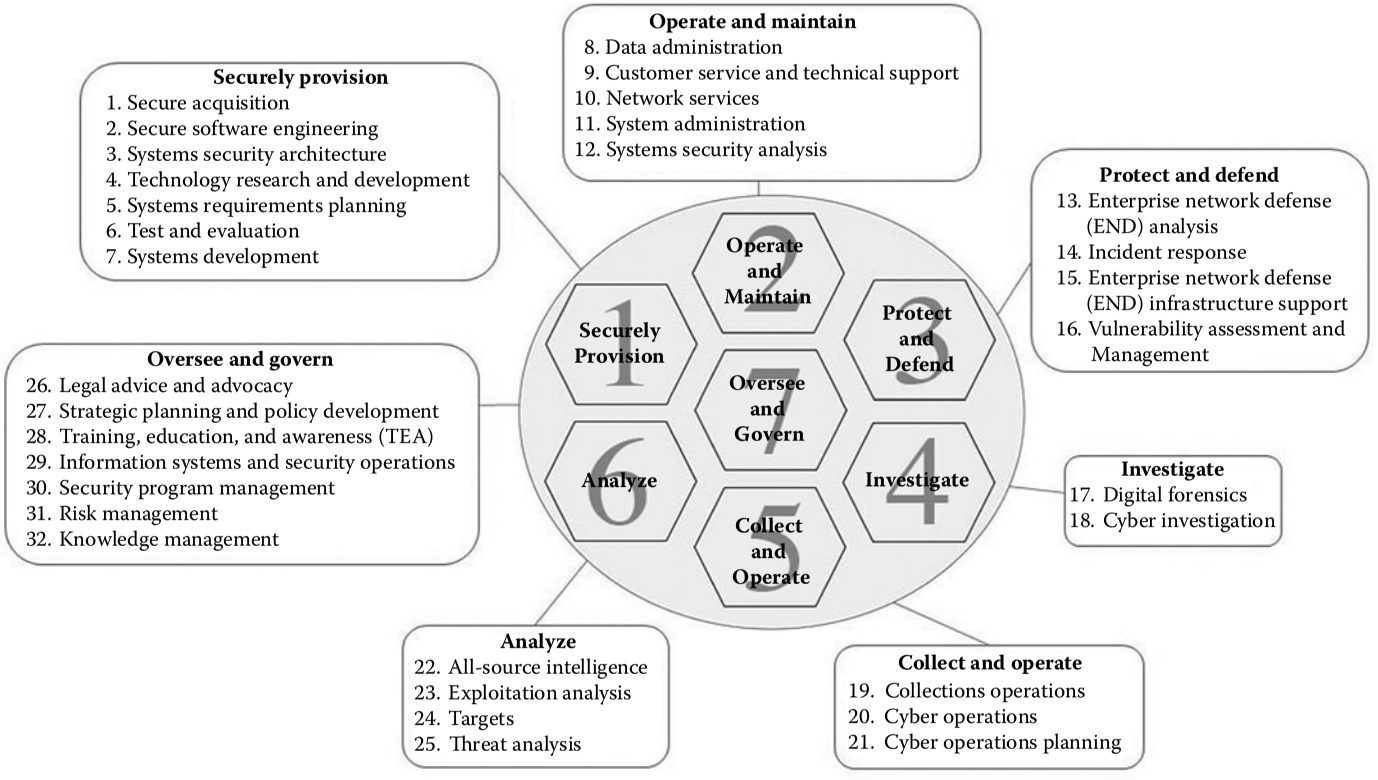

Figure 1.5 Sample job titles that lie within the 32 specialty areas as examples of common work functions.

Knowledge Area 1: Securely Provision

Securely provision encompasses those areas that are responsible for conceptualizing, designing, and building secure IT systems. In essence, these are the workforce roles who are responsible for some aspect of system and software development and maintenance. Securely provision contains seven specialty areas. These areas primarily lie in the academic and professional domain of software and systems engineering. Figure 1.6 shows the relationship between the securely provision general knowledge area, the specialty areas, and their corresponding roles.

The specialty areas that fall within securely provision are not usually considered to be part of traditional information security practice, at least in academe, because the securely provision areas concentrate more on the system itself than the information that it transmits.

Nevertheless, since most exploits target development and maintenance problems, the specialty areas of securely provision are among the most important aspects of the security roles in a modern organization. The specialty areas themselves illustrate the general focus and intent of the knowledge in securely provision. These specialty areas are discussed in the following sections.

Secure acquisition is the first specialty area in the securely provision knowledge area and it is an excellent way of illustrating the difference between the framework and any other model of the field. For the first time a major model of the discipline focuses on the management and support of the acquisition life cycle. Given our dependence on integration as a method of developing systems and the dependence of government and industry on commercial off-the-shelf (COTS) products, acquisition of secure products is a major national security issued.

The elements of acquisition include the necessary project setup and planning; the determination and documentation of the requirements; the selection; and procurement of ICT and cybersecurity products used in the organization's design, development, and maintenance of its infrastructure to minimize potential risks and vulnerabilities.

Acquisition oversees, evaluates, and supports the documentation, specification, contracting and oversight practices necessary to ensure a secure and correct new IT system or software product. It ensures that any purchase meets the organization's information assurance (IA) and security requirement. It ensures appropriate treatment of risk, compliance, and long-term operation of the product. Typical roles in this area include (NIST, 2014):

1. Chief information security officer (CISO)
2. Contracting officer (CO)
3. Contracting officer technical representative (COTR)
4. IT director

Secure software engineering is probably the most clearly recognized specialty area in this group. This is the area where the classic development and maintenance

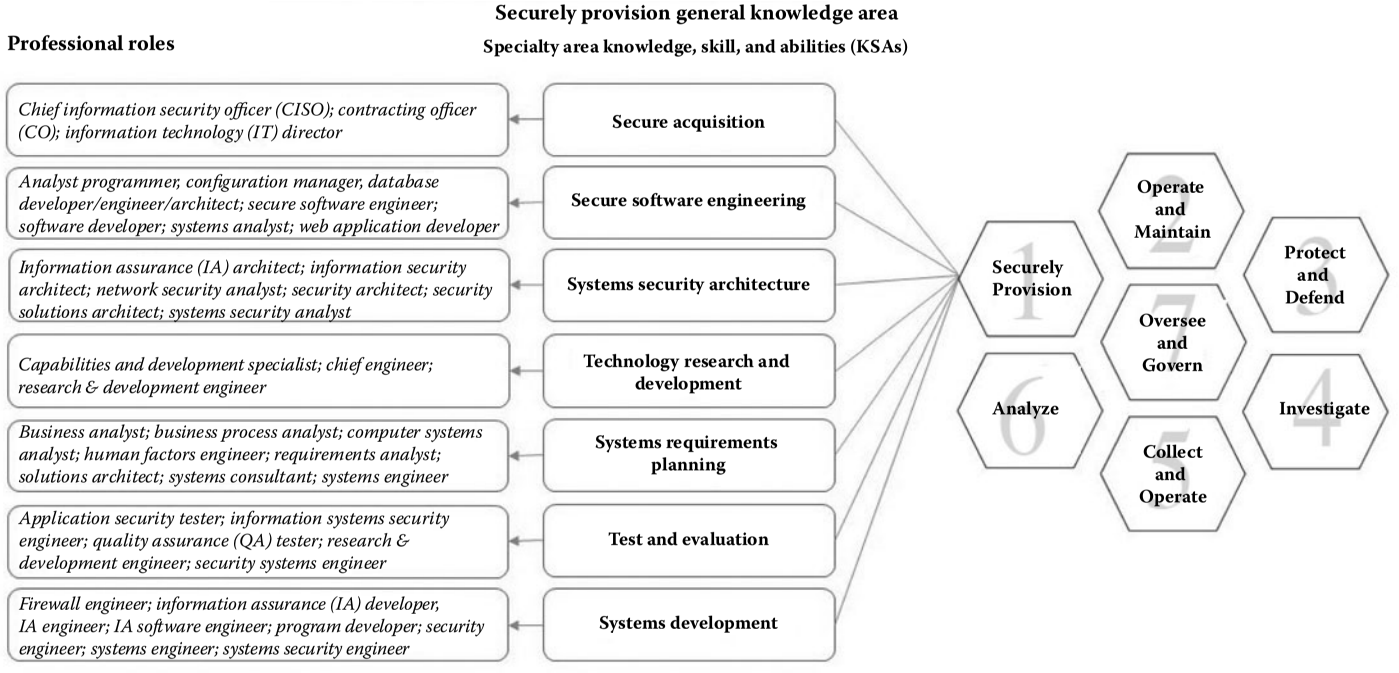

Figure 1.6 The relationship between the securely provision general knowledge area, the specialty areas, and their corresponding roles.

professionals work. And elements of this area have been well-recognized industrial roles for at least 50 years.

This is the area, which is primarily responsible for developing and coding new or for modifying existing computer applications, software, or specialized utility programs. Practitioners follow software assurance best practices that have emerged in the field over the past 25 years (NIST, 2014). Typical roles within this category include:

1. Analyst programmer
2. Computer programmer
3. Configuration manager
4. Database developer/engineer/architect
5. IA engineer
6. IA software developer
7. IA software engineer
8. Research & development engineer
9. Secure software engineer
10. Security engineer
11. Software developer
12. Software engineer/architect
13. Systems analyst
14. Web application developer

Systems security architecture is the other traditional area of the field. This specialty area focuses on the first critical stages of the waterfall. The primary focus is at the requirements and design phases of the systems development life cycle. Since these two stages lay down the initial conceptualization of the product, they have a disproportionate degree of influence on the eventual security outcome.

The job roles in this specialty area include researching, defining and capturing, and describing the detailed technological and environmental conditions for eventual incorporation into the system and security designs and processes. Those conditions include incorporating such things as business and legal and regulatory requirements. Typical job roles within this specialty area include:

1. IA architect
2. Information security architect
3. Information systems security engineer
4. Network security analyst
5. Research & development engineer
6. Security architect
7. Security engineer
8. Security solutions architect
9. Systems engineer
10. Systems security analyst

Technology research and development is not the same as testing, which is another specialty area related to assurance. This specialty area is responsible for the development of a meaningfully correct application of the product within the business environment as well as its continuing evolution. As a consequence, the job roles in this specialty area tend to be focused in outwardly facing concept positions, rather than production.

This specialty area does the necessary testing and general assessment of the technology that is required to develop and enhance its capabilities. In that respect, it supports the integration process as well as providing support for the organizations' prototyping capability (NIST, 2014). Typical job titles include:

1. Capabilities and development specialist
2. Chief engineer
3. Research & development engineer

Systems requirements planning is the traditional requirements area of the software engineering body of knowledge (SWEBOK). The requirements and planning process is user oriented in that the focus is on evaluating and documenting the system and/or software functional requirements and the translation of those requirements into technical solutions. This phase drives the design and coding processes that are downstream from it. As such its job roles are normally outwardly focused. Roles in this specialty area include:

1. Business analyst
2. Business process analyst
3. Computer systems analyst
4. Human factors engineer
5. Requirements analyst
6. Solutions architect
7. Systems consultant
8. Systems engineer

Test and evaluation is another traditional area of the SWEBOK. This area does the testing and assurance necessary to ensure a functionally correct and secure product. In that respect, professionals in this area perform formal testing of a system and/or software product with the aim of evaluating its compliance with specifications and requirements.

The focus of the jobs in this role is on the application of classic principles and methods in the planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT (NIST, 2014). Job roles in this category include:

1. Application security tester
2. Information systems security engineer

3. Quality assurance (QA) tester
4. Research & development engineer
5. Research & development research engineer
6. Security systems engineer
7. Software QA engineer
8. Software quality engineer
9. Systems engineer
10. Testing and evaluation specialist

Systems development is the classic development role. The job roles in this category fall within the traditional waterfall life cycle model. And they have been part of formal IT work since the beginning of the field. Within the security universe the focus of the role tends to be on security other than functional assurance. As a result, the roles themselves tend to have titles such as the following:

1. Firewall engineer
2. IA developer
3. IA engineer
4. IA software engineer
5. Information systems security engineer
6. Program developer
7. Security engineer
8. Systems engineer
9. Systems security engineer

Knowledge Area 2: Operate and Maintain

As shown in Figure 1.7, the specialty areas in this domain comprise the traditional areas of IT operation. These specialty areas ensure effectual and capable execution of a conventional IT function. They perform the classic support, administrative, and maintenance activities necessary to ensure correct and effective system performance as well as a sufficient and proper level of security.

In essence, these are the workforce roles that are responsible for the secure day-to-day operation of the IT function. Operate and maintain also has seven specialty areas. These areas primarily lie in the academic and professional domain of system management.

The specialty areas that fall within operate and maintain are at the heart of traditional information security best.

From the beginning the operate and maintain specialty areas have provided the necessary assurance of a desired level of system performance. Thus, the specialty areas of operate and maintain might be considered to be the most visible aspects of cybersecurity in a modern organization. The specialty areas themselves illustrate

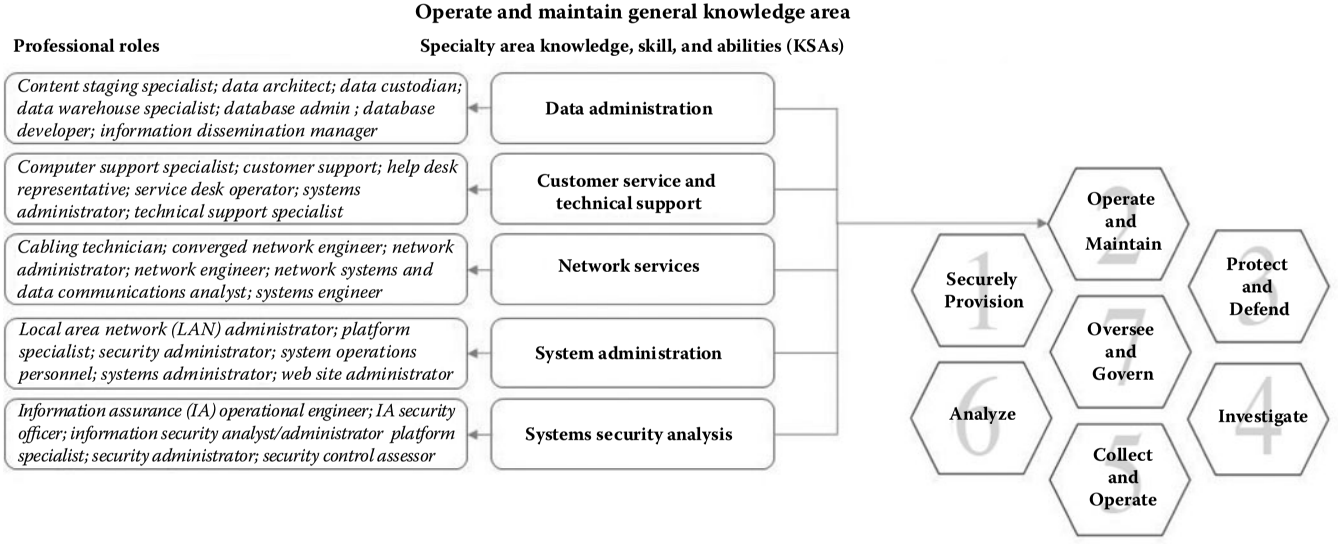

Figure 1.7 The relationship between the operate and maintain general knowledge area, the specialty areas, and their corresponding roles.

the general focus and intent of the knowledge in operate and maintain. These specialty areas are discussed in the following sections.

Data administration. Since information derives from data, this role is essentially the one that ensures the general integrity requirement. This role oversees the organization's databases. It develops and administers those databases and/or the data management systems that allow for the storage, query, and utilization of that data (NIST, 2014). Job roles within this specialty area reflect that development and oversight responsibility:

1. Content staging specialist
2. Data architect
3. Data custodian
4. Data manager
5. Data warehouse specialist
6. Database administrator
7. Database developer
8. Database engineer/architect
9. Information dissemination manager
10. Systems operations personnel

Customer service and technical support. Because user error is one of the primary causes of breach and unauthorized access, this humble area is among the most important and frequently overlooked elements of cybersecurity work. The general activities in this area include troubleshooting of problems as they arise in day-to-day operation. This area also installs, configures, troubleshoots, and provides maintenance of applications with a security requirement or focus. More importantly it is also responsible for executing and (potentially) escalating routine training activities that might arise as a result of routine business operation. Thus, the job roles in this specialty area include such business facing activities as

1. Computer support specialist
2. Customer support
3. Help desk representative
4. Service desk operator
5. Systems administrator
6. Technical support specialist
7. User support specialist

Network services. This specialty area comprises the classic network management function. This is a day-to-day operational, rather than a specific security-oriented function. It performs all of the essential, routine network and firewall installation, configuration, testing, operational, maintenance, and management activities.

That includes responsibility for the hardware and software that allows the sharing and transmission of networked information. The security focus is reflected in the job roles that comprise this specialty area:

1. Cabling technician
2. Converged network engineer
3. Network administrator
4. Network analyst
5. Network designer
6. Network engineer
7. Network systems and data communications
8. Analyst
9. Network systems engineer
10. Systems engineer
11. Telecommunications engineer/personnel/specialist

System administration. This is another one of the classic functions in the cybersecurity universe. Proper system administration ensures the secure operation of the system, its software, and networks. Consequently, the job roles in this specialty area are the ones responsible for the deployment, installation, configuration, and troubleshooting of all of the internal functioning and external communication aspects, both hardware and software, of the information system.

The aim of the job roles in this specialty area is to ensure the confidentiality, integrity, and availability of the data within the system. Job roles in this specialty area manage user accounts, and install and assure operational patches. They are specifically responsible for the classic security functions of access control, password, and account creation and privilege assignment, monitoring, and administration.

1. Local area network (LAN) administrator
2. Platform specialist
3. Security administrator
4. Server administrator
5. System operations personnel
6. Systems administrator
7. Web site administrator

Systems security analysis. This narrowly focused specialty area contains the job roles specifically responsible for ensuring the correctness and integrity of the system and the information it contains and processes. In that respect, the roles in this specialty area encompass the classic areas of traditional information security work.

Thus, the job roles tend to be focused on the integration and testing of new artifacts into the overall system structure along with the day-to-day oversight, analysis,

and the maintenance of system integrity and security. Jobs in this specialty area include:

1. IA operational engineer
2. IA security officer
3. Information security analyst/administrator
4. Information security manager
5. Information security specialist
6. Information systems security engineer
7. Information systems security manager (ISSM)
8. Platform specialist
9. Security administrator
10. Security analyst
11. Security control assessor
12. Security engineer

Knowledge Area 3: Protect and Defend

Many people believe that the specialty areas in this domain comprise the entire field of cybersecurity, because the protect and defend knowledge area encompasses all of those specialty areas that ensure effective data transmission, network operations and network security, as shown in Figure 1.8. The job roles within these specialties normally perform the classic network monitoring, administrative, and protection functions required to ensure trusted system and software performance within whatever security parameters the organization sets.

Consequently these are the workforce roles that are responsible for the trusted ongoing functioning and management of the network. The specialty areas within protect and defend are responsible for identification, analysis, and mitigation of all identifiable threats to internal IT systems or networks. Protect and defend has seven specialty areas. These areas primarily lie in the academic and professional domain of network operations/network security.

The specialty areas that fall within protect and defend are the classic information security roles. Those roles have always ensured the organization's desired level of trust in its networks and the information they transmit. Thus, the specialty areas of protect and defend might be considered to be the most commonly understood aspects of cybersecurity among people in general. The specialty areas themselves illustrate the general focus and intent of the knowledge in protect and defend. These specialty areas are discussed in the following sections.

Enterprise network defense (END) analysis. This is the traditional network security specialty area. The job roles within this area are all responsible for some aspect of enterprise-wide network defense. These roles collect information through electronic and behavioral means that will allow the organization to monitor the entire network for incidents, respond appropriately when an incident occurs, and

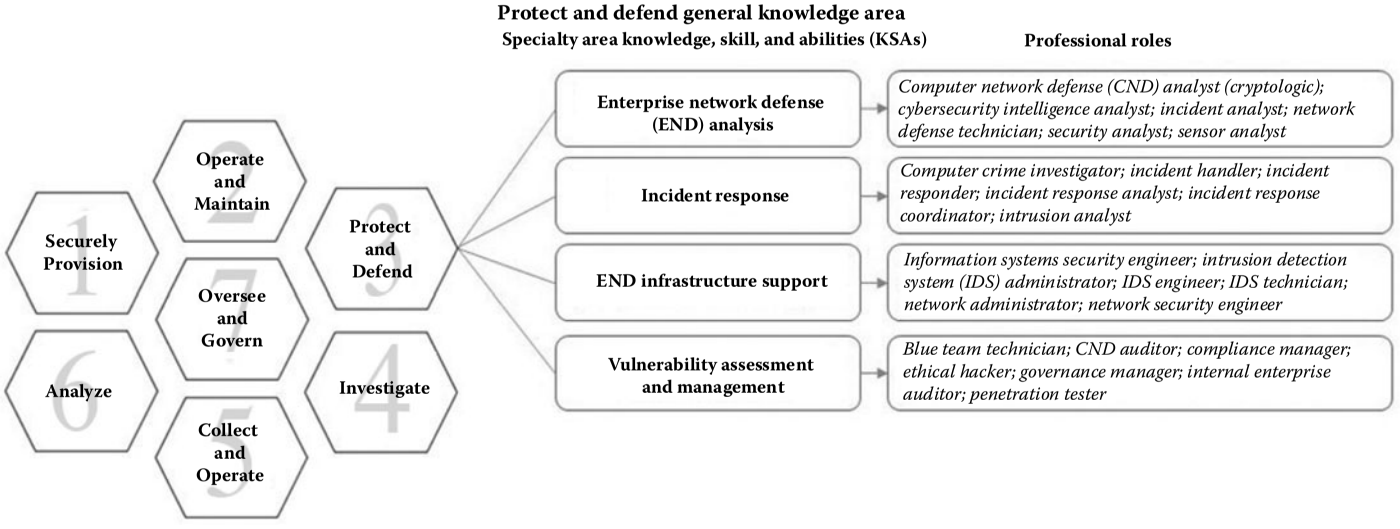

Figure 1.8 The relationship between the protect and defend general knowledge area, the specialty areas, and their corresponding roles.

document the occurrence for further analysis. The aim of all of these roles is to protect some aspect of the organization's information systems and/or their attached networks from threats.

1. Computer network defense (CND) analyst (cryptologic)
2. Cybersecurity intelligence analyst
3. Focused operations analyst
4. Incident analyst
5. Network defense technician
6. Network security engineer
7. Security analyst
8. Security operator
9. Sensor analyst

Incident response. This is perhaps the quintessential information security specialty area. The general aim of the incident response specialty areas is to respond to identified incidents as they occur. The goal is to mitigate any potential harm to the system or its attached networks. Both immediate and potential threats fall within the responsibility of this specialty area.

The job roles in this specialty area investigates and analyzes all relevant response options, prepares, and completes a set of response and recovery alternatives for each foreseeable threat. The aim is to maximize the survival of all systems and networks that fall within the assigned area of responsibility of this domain. Job roles include:

1. Computer crime investigator
2. Incident handler
3. Incident responder
4. Incident response analyst
5. Incident response coordinator
6. Intrusion analyst

END infrastructure support. This is an operational specialty area rather than one oriented specifically to network defense. It primarily monitors network operations in order to actively remediate any unauthorized activities that might be detected.

The job roles within this specialty area are responsible for the testing, implementation, deployment, sustainment, documentation, and management of all hardware and software network and resources that ensure adequate CND. Examples of job roles within this specialty area include:

1. Information systems security engineer
2. IDS administrator
3. IDS engineer
4. IDS technician

5. Network administrator
6. Network analyst
7. Network security engineer
8. Network security specialist
9. Security analyst
10. Security engineer
11. Security specialist
12. Systems security engineer

Vulnerability assessment and management. This is the network security analysis function. The job roles within this specialty area are specifically oriented toward the assessment and analysis of threats and vulnerabilities. The aim of the job roles in this specialty area is to identify and document any nonconformity with acceptable configuration norms or enterprise or local policies. Job roles within this specialty area include such functions as the following:

1. Blue team technician
2. Certified TEMPEST1 professional
3. Certified TEMPEST1 technical authority
4. Close access technician
5. CND auditor
6. Compliance manager
7. Ethical hacker
8. Governance manager
9. Information security engineer
10. Internal enterprise auditor
11. Penetration tester
12. Red team technician
13. Reverse engineer
14. Risk/vulnerability analyst
15. Technical surveillance countermeasures
16. Technician
17. Vulnerability manager

Knowledge Area 4: Investigate

The investigate knowledge area is a narrow aspect of the field that is primarily focused on after-the-fact investigation of incidents and other cyber-related events, such as crimes, intrusions, or harm caused to systems, networks. As the name suggests, the investigate knowledge area, shown in Figure 1.9, contains the job roles that obtain and analyze digital evidence to support evaluations of incidents that have occurred, as well as make recommendations about the ongoing performance of security operations.

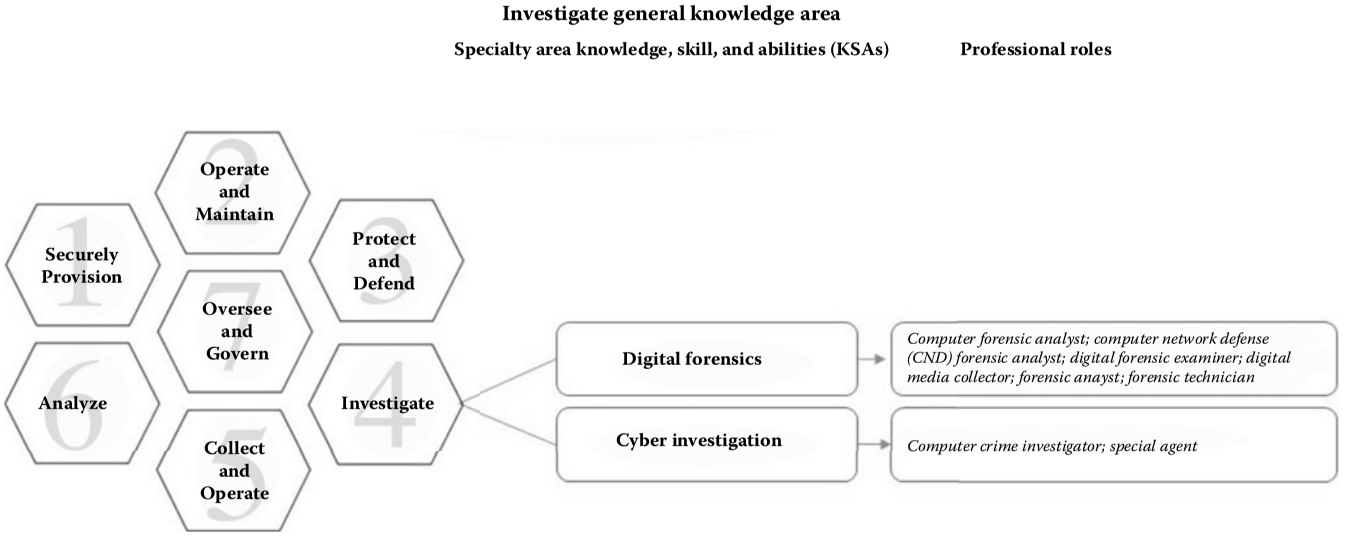

Figure 1.9 The relationship between the investigate general knowledge area, the specialty areas, and their corresponding roles.