CYBERSECURITY WORKFORCE HANDBOOK

A Practical Guide to Managing Your Workforce

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

ABSTRACT

This handbook is a practical guide to the management of the cybersecurity workforce within an enterprise, designed for executives, IT and security managers, and HR professionals. From high-level strategy development to workforce planning and ongoing governance, it provides step-by-step instructions on how to build a workforce that is oriented on implementing cybersecurity best practices. By providing a clear linkage between a common workforce taxonomy (National Initiative for Cybersecurity Education) and a set of prioritized actions for securing data and systems (Critical Security Controls), this handbook enables an enterprise to improve its cybersecurity by maximizing the impact of its most important resource- people.

Council on CyberSecurity

1700 N. Moore Street, Suite 2100, Arlington, VA 22209

+1 703-600-1935 | www.counciloncybersecurity.org

This material is based on research sponsored by Air Force Research Laboratory under agreement number FA8750-12-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

Additional support for this project has been provided by the Founding Members of the Council on CyberSecurity:

Cybersecurity Workforce Handbook

TABLE OF CONTENTS

1 INTRODUCTION

CONTEXT

The urgent need to better secure data and systems becomes more obvious each day. Digital assets, including the critical infrastructures foundational to a safe and secure nation, are under constant attack. On the whole, enterprises lack the knowledge, training and tools to establish effective, sustainable defense.

> *"Despite the growing space and sophistication of cyber threats… there are not enough people equipped with the appropriate knowledge, skills and abilities to protect the information technology for strategic advantage."*
> -Professionalizing Cybersecurity: A Path to Universal Standards and Status

The persistent vulnerability of individuals, enterprises and entire industry sectors to a range of malefactors, from common criminals to terrorist networks and nation-states, is an unavoidable reality. In 2012, 56 companies participating in a Ponemon Institute study reported 102 successful attacks per week, or 1.8 successful attack per week, per organization[i]. By most measures, the advantage is currently with the attacker, who enjoys easy access to tools and tactics, low cost to carry out attacks, access to a broad network of fellow hackers with whom to share tips, little fear of identification, and even less concern about capture or punishment.

It has become clear that traditional reliance on information technology (IT) specialists alone cannot protect an enterprise from cybersecurity threats. A comprehensive approach-one that integrates best practice across policy, technology and people-is necessary to increase the security posture of organizations and shift the balance in favor of the defender. Of critical importance are the capabilities of the people responsible for managing information systems, hiring cybersecurity talent, establishing corporate policy, and building corporate culture. These individuals represent a diverse set of functions, from non-technical executives and board directors, to cybersecurity experts with highly technical skills. The proper management of employees integral to the cybersecurity workforce is an essential component of an effective enterprise cybersecurity strategy.

CHALLENGES

There are many challenges inherent in cybersecurity workforce management, due largely to the relative newness and complexity of the field. Lack of clarity and consistency is still the norm- from job role definitions, to competency models, to training, education and certification standards, to the ability to assess those skills

necessary for effective job performance. Managers of cybersecurity functions- often embodied in the Chief Information Security Officer (CISO) but also inclusive of Chief Information Officers (CIO), Chief Security Officers (CSO), Chief Risk Officers (CRO), and myriad IT and security managers- lack planning tools for this work. Contrasted with highly-professionalized and regulated fields such as medicine, law and accounting, the cybersecurity profession remains a milieu of functions spread across myriad roles with murky definitions and limited ability to predict performance.

Lack of…

Clarity & consistency

Funding

Understanding by non-technical leaders

Training

HR planning tools

Lack of resource allocation is a downstream symptom of the lack of clarity and consistency which makes it harder for cybersecurity managers to articulate needs, including critical budget requirements, to non-technical managers. This further exacerbates the overall problem. The result? Underfunded and understaffed cybersecurity teams.

Lack of understanding is typical of non-technical leaders who have not been trained how to integrate risk management with workforce management. This is not surprising, as risk management is a broad discipline, primarily exercised within executive management functions, including board governance, as well as within finance and operations. It is seldom appropriately linked to the human resources (HR) function. HR is usually brought in later in the process, when these other functions have already established specific needs for qualified personnel within their departments. A comprehensive approach to risk management *through* workforce planning, an area traditionally managed by HR, is not the norm.

In the case of cybersecurity, the challenge and opportunity exists to not only properly staff specific IT and security functions with top talent, but to further enable broader cybersecurity activities by organizing and deploying the broader workforce in a cybersecurity-oriented, prioritized way. Workforce planning itself can become a security enabler. This requires a clear linkage between workforce planning and prioritized action for securing the enterprise.

> *"Corporate executives often lack a complete understanding of their companies' security needs and their inability to locate enough qualified security professionals, which leads to more frequent and costly data breaches."*
> -Professionalizing Cybersecurity: A Path to Universal Standards and Status

Lack of training and reference resources make it hard for HR professionals to fulfill their role of supporting enterprise workforce needs. While there are countless workforce planning tools and templates available today, they are overwhelmingly process-oriented. They serve as guides for navigating the planning process in a structured way, but most lack guidelines specific to an industry sector, profession or enterprise function- like cybersecurity.

Addressing these challenges requires an approach to managing the cybersecurity workforce which integrates enterprise strategy and risk management with HR best practices, aligns with existing frameworks for organizing the cybersecurity workforce, and is oriented on prioritized action for securing the enterprise.

SOLUTION

This handbook is designed as a ready reference for executives, hiring managers (often in IT and security functions) and HR professionals charged with managing the planning, sourcing, hiring, training, development, career progression and sustainment of the cybersecurity workforce. It seeks to fill the gap between the disciplines of workforce planning and cybersecurity planning, aligning the workforce to enterprise security. Beyond the management of the few individuals designated as cybersecurity professionals, this effort extends to other IT and security functions, and even more broadly to the entire enterprise workforce, recognizing that every employee plays a part in securing data, systems and infrastructure.

> *"81% believe that if the right investments in people, process and technologies were in place, their organizations would be better able to mitigate all future security breaches."*
> -2014 Ponemon Institute Research Report

This handbook is designed to provide the following:

- Guidelines for the deployment of critical (and limited) cybersecurity professionals in a prioritized manner, aligned to best practice
- Steps to link cybersecurity planning with workforce planning
- Definitions to clarify roles and functional responsibilities
- A basis for consistency across enterprises and across industry sectors
- A contribution toward the professionalization of the cybersecurity workforce through increased predictability in job roles and career pathways

APPROACH

The strategic management of the workforce in any enterprise must be based upon a clear understanding of, and linkage to, enterprise strategy. In the case of securing data, systems and infrastructure, this means that workforce planning must align with a comprehensive cybersecurity strategy. While this field has often been considered a subset of the CIO function and the IT department, it is now clear that an enterprise cannot be properly secured without a broader effort.

Therefore, the first step is to ensure that the enterprise is focused on prioritized action. For this, the foundation is provided by the Critical Controls for Effective Cyber Defense (Critical Controls), also known as the Top 20 (detailed in the next chapter). The Critical Controls are the result of an ongoing collaboration among leading technologists, academics and policymakers in the field. They are a recommended set of actions for cyber defense which provide specific and actionable ways to prevent and mitigate the most pervasive attacks. They are linked to existing standards and frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, providing a way to focus limited resources on steps with the greatest impact.

> *"Often, we find that the CISO or IT risk officers are valiantly fighting the cyber battle, with limited support from the executive management team or the broader IT team."*
> –Deloitte Center for Financial Services

At the same time, the current workforce must be viewed in a structured way. The National Initiative for Cybersecurity Education (NICE), which was developed by NIST, has organized all cybersecurity functions into seven categories and 31 specialty areas, with associated competencies, tasks and knowledge, skills and abilities (KSAs). While there are countless variations of job titles throughout the marketplace, the NICE framework provides a stable reference point for examining cybersecurity jobs.

Mapping of NICE specialty areas to the Critical Controls provides a way to link jobs to prioritize enterprise action. Based on this, specific recommendations are made on which technical roles to prioritize, what the job descriptions should look like, placement of these roles within the enterprise, responsibilities and authorities of these roles, management oversight, and the tasks necessary for non-technical employees to accomplish. The result is a set of guidelines applicable to enterprises of varying size and complexity, across industry sectors and geographic regions.

2 FOUNDATIONAL ELEMENTS

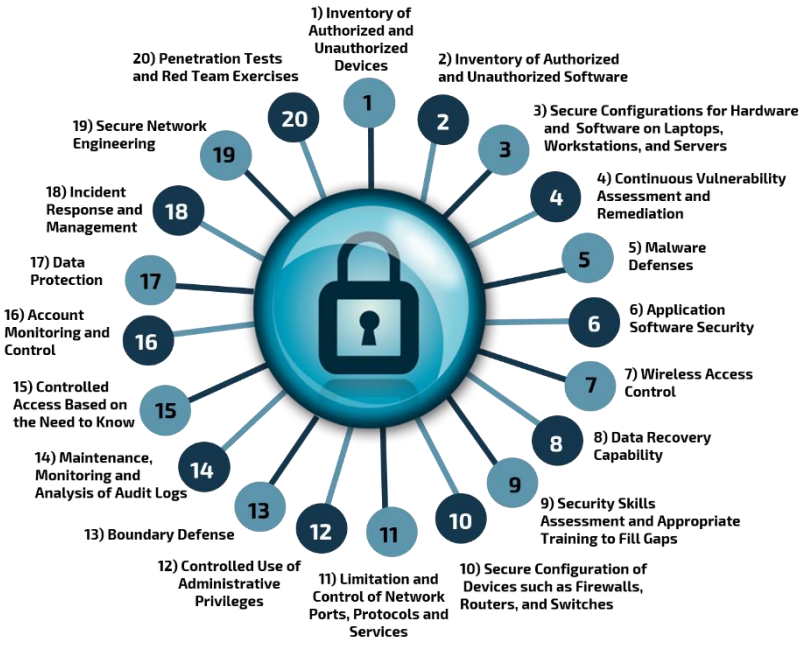
BUILDING BLOCKS

Several essential building blocks comprise this handbook's approach to cybersecurity workforce management. The Controls provide the focal point for enterprise cybersecurity strategy and, by extension, workforce management. They serve as the desired end state for the activities of the workforce. At the same time, the NICE framework provides a reference framework and taxonomy for discussing the many roles in cybersecurity.

While there are numerous other frameworks and standards which are applicable to this effort, the Critical Controls and the NICE framework were selected because they provide a concise, focused means to address both fronts- cybersecurity itself, and the cybersecurity workforce. This does not preclude the use of other references, either in this handbook or in the workforce management efforts which it supports. Additional references are provided in Appendix D.

CRITICAL SECURITY CONTROLS

More so now than at any point in the last few decades, defenders have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, configuration guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. There has been a rapid growth of numerous threat information feeds, reports, tools, alert services, standards, and threat sharing schemes. And to tie it all together, enterprises are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth.



There is a near-infinite list of "good things" for every enterprise to do and to know to improve the security of cyberspace, but it's seldom clear what to prioritize. This overload of defensive support is a "Fog of More"- more options, more tools, more knowledge, more advice, and more

requirements... but not always more security. What is needed is a way to organize and prioritize activity around a set of actions known to be effective in addressing most threats. This was the impetus behind the development of, and the continued refinement of, the Critical Controls.

Initially developed in 2008 by a consortium of U.S. federal agencies led by the National Security Agency, the Critical Controls are currently maintained by the Council on CyberSecurity (Council), which engages an international community to:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and the use of tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- Map the Critical Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Share tools, working aids, and translations;
- Identify common problems (like internal assessment, building implementation roadmaps) and solve them as a community instead of alone

The Critical Controls, listed in Figure 1, are actions that encompass elements of technology, policy and workforce management:

CRITICAL CONTROL	DESCRIPTION
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Malware Defenses
6	Application Software Security
7	Wireless Access Control
8	Data Recovery Capability
9	Security Skills Assessment and Appropriate Training to Fill Gaps
10	Secure Configurations for Network Devices
11	Limitation and Control of Network Ports, Protocols, and Services
12	Controlled Use of Administrative Privileges
13	Boundary Defense
14	Maintenance, Monitoring, and Analysis of Audit Logs
15	Controlled Access Based on the Need to Know
16	Account Monitoring and Control
17	Data Protection
18	Incident Response and Management
19	Secure Network Engineering
20	Penetration Tests and Red Team Exercises

Figure 1 - List of Critical Security Controls, v5.0

These Critical Controls do not comprise new standards, per se. Rather, they prioritize existing controls defined in existing standards. For example, the actions defined by the Controls are a subset of the National Institute of Standards and Technology (NIST) publication SP 800-53, a comprehensive catalogue of controls. The Critical Controls

do not attempt to replace the NIST Risk Management Framework[ii]. Instead they prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Critical Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.

For these reasons, the Critical Controls are presented here as foundational elements of cybersecurity, and the basis for workforce management. For more information, visit the Council's website at http://www.counciloncybersecurity.org/critical-controls/.

NICE FRAMEWORK

The National Initiative for Cybersecurity Education (NICE) is a program of NIST, designed to address the shortage of qualified cybersecurity professionals. Through their National Cybersecurity Workforce Framework (NICE framework), NICE provides a common taxonomy and reference framework for workforce management across all cybersecurity roles. Defining the cybersecurity profession, through the use of standardized terms and language, facilitates the ability to educate, recruit, train, develop and retain a capable workforce.

Categories	Specialty Areas						
Operation & Maintain	Data Administration	Knowledge Management	Customer Service & Technical Support	Network Services	System Administration	Systems Security Analysis	
Protect & Defend	Computer Network Defense Analysis	Incident Response	Computer Network Defense Infrastructure Support	Vulnerability Assessment & Remediation			
Investigate	Digital Forensics	Investigations					
Collect & Operate	Collection Operations	Cyber Operations Planning	Cyber Operations				
Analyze	Threat Analysis	Exploitation Analysis	All Source Intelligence	Targets			
Securely Provision	Information Assurance Compliance	Software Assurance & Security Engineering	Systems Security Architecture	Technology Research & Development	Systems Requirements Planning	Test & Evaluation	Systems Development
Oversight & Development	Legal Advice & Advocacy	Education & Training	Strategic Planning & Policy Development	Information System Security Operations	Security Program Management		

Figure 2 - NICE Categories

The NICE framework is comprised of seven job categories, based on logical groupings of functions within the cybersecurity lifecycle.

Across these categories are 31 specialty areas, which are specific roles with associated competencies, tasks and KSAs on a more detailed level. Additionally, the specialty areas are linked to common job titles found in the job market. More information on the framework can be found on the National Initiative for Cybersecurity Careers and Studies (NICCS) portal at niccs.us-cert.gov.

Mapping the NICE framework to Critical Security Controls links job roles and KSAs to prioritized cybersecurity actions. This analysis was validated by a panel of Subject Matter Experts (SMEs) convened by the Council.

3 WORKFORCE MANAGEMENT CYCLE

THE MANAGEMENT CYCLE

Enterprises of every size and complexity, from small, home-based businesses to large, multinational corporations and government agencies, need to protect their data, systems and infrastructure. This requires an effective cybersecurity strategy and a solid workforce plan. The steps to achieve this begins with a problematic current situation (threats and vulnerabilities) and leads to with an effective ongoing governance of Critical Controls-based practices, with a workforce deployed to implement and maintain them.

The Workforce Management Cycle is a sustainable and self-reinforcing process for cybersecurity workforce management:

Figure 3- Workforce Management Cycle

Each of these steps contain basic actions that an enterprise can take, and are associated with common, methodologies and frameworks. Notably, the Workforce Management Cycle leverages actions which are familiar to any enterprise:

- Market research- Get a sense for what's happening out there
- Strategic planning- Figure out what needs to be done
- Workforce planning- Organize a team to get the job done
- Corporate governance- Maintain management oversight

This process integrates these actions with cybersecurity best practices to create a cohesive approach to improving enterprise security.

UNDERSTAND THREATS & VULNERABILITIES

It is vital for every enterprise to have an understanding of threats and vulnerabilities. Numerous studies have shown that though leaders are becoming more aware of cyber risk they are often still unaware of the extent to which their particular organization may be the target of cyber attacks. Lloyd's Risk Index 2013, the product of a biennial survey of the risk priorities and attitudes of business leaders from across the globe, shows that cyber risk has risen from the 20th ranked risk in 2009 to the 12th ranked risk in 2011 and is now the 3rd ranked risk overall in the world (and is ranked 2nd in the United States)[iii]. High profile cyber incidents have more than likely contributed to the increased awareness of cyber risk in general but leaders remain mostly unaware of what specific cyber threats facing their particular enterprise. In a 2014 survey of IT and IT security professionals in the United States and United Kingdom, conducted by the Ponemon Institute, only 20% of respondents regularly communicate with their management about cyber threats[iv]. These statistics help showcase the need for a greater awareness of the general dangers faced by all enterprises, along with a basic understanding of the types of threats and vulnerabilities which attend companies of specific profiles.

> *"Get the group of stakeholders together who own the information assets, that group needs to work with the risk and security specialists to assess the specific threats the organization is likely to be facing.*
> – Mark Fishleigh, Director, BAE Systems Detica

Two simple actions can increase enterprise awareness of general and specific threats and vulnerabilities:

- Build awareness by signing up for alerts via US-CERT at www.us-cert.gov, Information Sharing Analysis Centers (ISAC's) at www.isaccouncil.org, industry groups, cybersecurity product and service providers

TIP: This doesn't require spending limited funds; most of these resources are free.

- Leverage available tools to conduct a basic vulnerability assessment to identify weaknesses by downloading DHS Cyber Security Evaluation Tool at ics-cert.us-cert.gov/Downloading-and-Installing-CSET

DEVELOP CYBERSECURITY STRATEGY

Substantial improvements to enterprise security can be achieved through integration of cybersecurity with overall enterprise strategy. The process to generate an enterprise-wide cybersecurity plan (even a rudimentary one) can have a big impact, even before the plan is implemented. By demonstrating senior leadership commitment to security, involving key stakeholders from various business units and functions, and working together to understand cybersecurity- a topic often ignored or avoided- a cohesive planning process can provide common understanding of what the enterprise is doing to protect itself. This is where the Critical Controls play a major role by providing a ready-made, expert-vetted list of things the enterprise should do.

TIP: Leadership is fundamental. The personal involvement of senior leaders is a must for this to work!

Developing a cybersecurity strategy includes the following actions:

- Follow the basic steps of the NIST Cybersecurity Framework
- Take immediate steps to implement the First Five Quick Wins (of the Critical Controls)
- Identify remaining Critical Controls to prioritize, based on enterprise risk profile
- Identify strong leaders to ensure implementation

LINK ROLES & CONTROLS

Once a plan is in place to improve security by implementing Critical Controls, the roles necessary to implement them need to be identified. A 2014 SANS Institute survey indicated insufficient staffing or personal resources as the most significant barrier to implementing the Critical Controls[v]. As described earlier, the starting point for any examination of the cybersecurity workforce is the NICE framework. By conducting an inventory of existing roles, linking Critical Controls to appropriate roles and understanding where there are overlaps, the workforce structure can be aligned with the cybersecurity plan.

Linking roles to Critical Controls includes the following actions:

- Inventory the current workforce to identify how existing roles map to the NICE framework- this includes functions being performed by employees of various formal titles and roles
- Leverage the individual Critical Controls mappings (Appendix C) to identify the roles needed for implementation of the enterprise cybersecurity plan

- Leverage the Heat Map (Appendix B) to identify overlaps, redundancies and synergies so that limited resources can be applied for maximum benefit

DEFINE WORKFORCE REQUIREMENTS

The linkage of roles to Critical Controls provides the cornerstone for an enterprise-wide workforce plan. The 2014 SANS Institute survey noted the disconnect between operational and security silos as the third leading barrier to implementation of Critical Controls[vi]. Because many prioritized cybersecurity actions (i.e. Critical Controls) require consistent execution of tasks by roles which are not specifically cybersecurity (i.e. IT operations, IT line managers, information security or information assurance), a broader plan must be developed around the roles-to-Critical Controls linkage. This way, the resulting workforce plan includes tasks for nearly everyone in the enterprise, from frontline individual contributors to managers to IT staff to executive leadership.

Defining workforce requirements includes the following actions:

- Leverage the Essential Tasks Pyramid (Figure 7, page 40) to identify common tasks across the enterprise by degree of responsibility for data and system
- Build upon the mapping of roles to Critical Controls to identify the specific roles which must be deployed (or redeployed) within the organization
- Develop and implement a plan for building a security-oriented culture through leadership engagement

OUTLINE SOURCING PLAN

For any workforce plan, consideration must be given to how various roles are sourced, determining who will provide the capabilities for each role and how these roles will be brought into the enterprise. For many large enterprises and federal government agencies, a determination must be made whether to hire these roles into the organization or address this need as a service delivered by an external provider. Meanwhile, most small and medium-sized businesses have no choice but to outsource many of these functions, due to a lack of internal expertise and resource constraints. How these roles are sourced can have a significant impact on the success of the cybersecurity strategy, so there must be a deliberate effort to understand these dynamics.

> *"Bringing in complementary outside resources can not only help to reduce costs, but also allow the business to free up resources to focus on higher priorities."*
> –Cisco Annual Security Report 2014

Outlining a sourcing plan includes the following actions:

- Conduct a gap analysis of cybersecurity expertise within the enterprise

- Identify which roles and associated skill sets can be developed internally and which require external sourcing
- Develop guidelines for how to manage functions which are outsourced

DEPLOY THE WORKFORCE

Because cybersecurity roles- like all roles within an enterprise- are finite resources, their proper deployment is essential. Deployment includes placement within an organization, assignment of responsibilities and authorities, and establishment of the reporting chain. When properly deployed, the workforce becomes a powerful enabler of effective security, hardening the enterprise against routine threats, better identifying specific attacks of greater danger, and responding in an effective manner. Poor deployment, meanwhile, can lead to a disjointed effort by employees who lack a common understanding of the problem and who are ill-equipped to handle emerging challenges.

Deploying the workforce includes the following actions:

- Leverage the Manpower Map (Appendix D) to properly place roles within the organizational structure
- Assign responsibilities in order to have clear accountability for functions, and to properly enable roles with the authority to get the job done
- Establish the reporting chain for maximum accountability and flexibility, as some reporting chains may not mirror the organization chart

MAINTAIN GOVERANCE

Once in place, both the cybersecurity strategy and its supporting workforce plan must be sustained through effective oversight. As distracted as organizations can become, no security plan can be successfully implemented without the direct involvement of executive leadership. Often at odds with the business-oriented needs of availability, efficiency and speed, better security requires deliberate effort. Effective governance includes tracking the progress and effectiveness of the program, ensuring sufficient funding, and capturing feedback for regular updates to the cybersecurity strategy and associated workforce plan.

Maintaining governance includes the following actions:

- Establish a cross-functional governance committee which reports directly to the Chief Executive Officer (CEO) or the board of directors
- Establish tracking mechanisms for the security plan, which includes metrics for the workforce plan
- Establish a cadence for updating the cybersecurity strategy and workforce plan

4 UNDERSTAND THREATS & VULNERABILITIES

BUILDING AWARENESS

Every enterprise- from home offices and small businesses to multinational corporations and federal government agencies- must develop an awareness of threats and vulnerabilities. This, in turn, means both an *appreciation* for threats and vulnerabilities in a general sense, and the establishment of mechanisms to maintain *current knowledge* of such threats and vulnerabilities.

> *"The increase in successful attacks brings with it media attention and citizen concern, but it is critically important that the public conversation we are now having not just be about one attack or one company… over time we often learn that the most widely reported victim was not the one hit hardest."*
> -Fran Rosch, Senior Vice President, Security Products & Services, Endpoint and Mobility, Symantec Corporation

The former has been difficult to attain but substantial progress has been made in the past few years. Several major studies have highlighted that, until recently, there existed a general lack of awareness and urgency when it comes to securing data and systems- particularly among senior executives.[vii] However, thanks to many recent high-profile breaches, and even the resignation of a prominent CEO due to a major data breach, the level of appreciation for the risk has increased significantly in a short amount of time.[viii] It is now clear to most boards and management teams that, like it or not, cybersecurity is a matter which must be addressed.

Maintaining current knowledge of specific dangers is a ceaseless project, but in following five tasks, an enterprise can learn the necessary background and put a process in place to stay informed of the ever-changing cybersecurity landscape.

TASK 1: BUILD FOUNDATIONAL KNOWLEDGE

Those responsible for data and systems within an enterprise- including leaders on the executive management team, as well as IT and cybersecurity managers- must have some basic knowledge about what cybersecurity is all about. This does not require in-depth technical knowledge[ix], but does include basic understanding of how information flows through the infrastructure, how it's stored and managed, how employees connect to information, what depends on this information (which, as will become quickly evident, is nearly everything), and how to use an end-user device (like a laptop or tablet) safely. It also includes understanding of privacy and intellectual property protection, relevant industry-specific regulations, and dependencies in the supply chain- the network of other entities with whom the enterprise is connected to

do its work. This is analogous to driving an automobile, which does not require extensive knowledge of mechanical engineering but does require knowledge of traffic laws and safety guidelines (like buckling a seatbelt). Similarly, an understanding of cybersecurity principles does not require a computer science degree but does require an understanding of its own guidelines for safe operation.

Suggested sources for developing this foundational knowledge include:

- DHS sources:
  - Stop.Think.Connect., www.dhs.gov/stopthinkconnect-get-informed
  - US-CERT Bulletins, www.us-cert.gov/ncas/bulletins
  - OnGuardOnline.gov, www.onguardonline.gov/
- NIST sources:
  - NIST Cybersecurity Framework, www.nist.gov/cyberframework/
  - NIST Risk Management Framework, csrc.nist.gov/groups/SMA/fisma/framework.html
- Non-profits:
  - Center for Internet Security, www.cisecurity.org/
  - National Cybersecurity Alliance, www.staysafeonline.org
  - Online Trust Alliance, otalliance.org/
- Training courses:
  - SANS Institute, www.sans.org/courses/
  - Cyber Aces, cyberaces.org/
- Vendor news/blogs:
  - SANS Security Resources, www.sans.org/security-resources/
  - SANS Newsletters, www.sans.org/newsletters/
  - Tripwire State of Security, www.tripwire.com/state-of-security/
  - Qualys Community, community.qualys.com/welcome
  - FireEye Blog, www.fireeye.com/blog/
  - Mandiant M-unition, www.mandiant.com/blog/

Initially, it may take a lot of effort to develop foundational knowledge. Like any body of knowledge, the initial building blocks are disconnected and appear disjointed, but with time and exposure, these building blocks begin to form outlines and contours upon which additional information will attach- all building a base of knowledge which can make any non-technical person a “smart user.”

TASK 2: TRACK EMERGING THREATS

The explosive growth in the number and variety of threats has led to the maturing of industry mechanisms for identifying, tracking, and categorizing these threats. An enterprise can substantially increase its awareness of threat vectors (major avenues of attack or means of causing damage), as well as specific threats (targeting very specific weaknesses in operating systems, network access points, etc.), by subscribing to threat reports which are published by government agencies and large providers of telecommunications, IT and cybersecurity services.

Major threat reports include:

- 2014 Verizon Data Breach Investigation Report (DBIR)
- Hewlett Packard CyberRisk Report 2013
- Cisco Annual Security Report 2014
- Trend Micro 2014 CyberThreat Defense Report
- Symantec 2014 Internet Security Threat Report
- FireEye Advanced Threat Report 2013

> *"45% of respondents indicated that the Board did not receive regular updates on the key issues concerning information security and privacy risk management."*
> –Harvard Business Review, "Meeting the Cyber Risk Challenge"

Increasingly, these threat reports are adhering to standard taxonomies for categorizing the threats, which in turn provide a way to analyze trends. Also, some reports, like the Verizon Data Breach Incident Report[x], provide useful tools for subsequent steps in the Workforce Management Cycle by linking major threat vectors to specific Critical Controls which would best mitigate them.

TASK 3: SHARE INFORMATION

When it comes to securing data and systems, and in particular critical infrastructure, no enterprise is an isolated actor. The dependence on infrastructure, like electricity and telecommunications, as well as networks of suppliers and buyers, link enterprises in common cause- even competitors in the same industry. It is in everyone's interest to reduce the impact of data breaches and system disruptions, and lower the costs of

> *"Overall, the costs and complexity of responding to incidents are increasing… the cost to investigate; the cost to understand business risks and contain incidents; the cost to manage notification to regulators, customers, and consumers; and the cost of litigation."*
> -Shane Sims, Principal, PricewaterhouseCoopers

cyber attacks as much as possible. In recognition of this need, there are now platforms for sharing information and collaborating in this endeavor.

- Information Sharing and Analysis Centers (ISAC)
  - Center for Internet Security, www.cisecurity.org/
  - Multi-State Information Sharing Analysis Center, msisac.cisecurity.org/
- Campaigns
  - National Cyber Hygiene Campaign, cisecurity.org/about/CyberCampaign2014.cfm

These platforms typically provide a set of benefits, including alerts to emerging threats focused on the particular sector, broader situational awareness of broad trends, sharing of best practices, and advocacy for the needs of the sector.

TASK 4: PERFORM ENTERPRISE RISK MANAGEMENT

Today in cybersecurity it's easy to see the failure of poor risk management in cases like the widely-publicized Target, JP Morgan, and Home Depot data breaches. News stories feature frequent accounts of "bad actors," including cyber gangs, terrorists and nation states. Every week there seems to be breach of a major enterprise.

> *"Only 20% of IT and IT security professional respondents regularly communicate with their management about cyber threats."*
> -Ponemon Institute, January 2014

Breaches are symptoms of not being able to pre-emptively account and plan for external risks. There are many resources available to assess one's security posture. Identification, analysis, and evaluation of threats and vulnerabilities (risk management) are the only way to assess the potential impact and implement necessary controls.

Internal corporate weaknesses receive less attention than massive data breaches or terrorist threats, but they encompass what is immediately under management control. Just like business operations, financial operations, and customer service operations, cybersecurity operations need a strong and educated workforce, which is the foundation for maturity and effectiveness overall. Having the right people in the right place with the right skills to do the right job will reduce exposure to attacks.

UNDERSTAND THREATS & VULNERABILITIES

A well-trained team can provide a comprehensive view of all the cybersecurity dangers the enterprise faces, from the most common areas (phishing attacks and software that needs updating) to new business programs, platforms and online services that need to be reviewed from a security perspective.

> *"Barriers to adopting and automating the Controls include insufficient staffing, lack of budget and silos between IT security and operations."*
> -SANS Institute Analyst Survey, September 2014

The process to manage enterprise risk, including cyber threats and vulnerabilities, has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is important during this stage to identify and record all risks.

Enterprise-wide cyber risk categories can be organized into the following areas:

1. Information exposure/loss: includes risks associated with the intentional or unintentional loss, theft, compromise, or disclosure of any type of sensitive department information or data
2. Unauthorized use: includes risks associated with the intentional or unintentional use of any type of sensitive department information or data information system, or processes/procedures by an unauthorized individual
3. Exposure to contaminated environments: includes risks associated with the intentional or unintentional exposure of any type of sensitive department cyber asset or information to potentially contaminated, mistrusted, or insecure environments that may adversely affect the confidentiality, integrity, or availability of the exposed cyber asset or information
4. Weak processes/unsecure operating environments: includes risks associated with the intentional or unintentional harm to any type of sensitive department information or data information system, or processes/procedures resulting from inadequate controls, either technical or manual
5. Loss of public confidence: includes risks associated with the intentional or unintentional harm to the reputation of the enterprise and/or its leadership and the confidence of the public or senior government officials in the enterprise's ability to conduct its mission effectively
6. Exposure to legal action: includes risks associated with financial or non-financial legal actions taken against the department and/or its leadership.

To minimize the risk of legal action, it is important to understand regulatory compliance. Some of the most-relevant standards bodies include:

- Payment Card Industry (PCI), www.pcisecuritystandards.org/

- Health Insurance Portability and Accountability Act (HIPAA), www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf
- International Standards Organization (ISO) 27001, www.iso.org/iso/home.html

TASK 5: CONDUCT A VULNERABILITY ASSESSMENT

In addition to an understanding of broader risks, including external threats and shared vulnerabilities, an enterprise should take steps to understand specific vulnerabilities within its own systems. This can be accomplished by several means:

- Install an automated vulnerability scanner
  - The non-profit Open Web Application Security Project (OWASP) has compiled a listing of scanners, www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
- Conduct a manual vulnerability assessment, which can be provided by external consulting firms

While the threat landscape is constantly evolving[xi] and no approach will provide a complete and perfect mapping of all risks, these tasks can provide a solid understanding of threats and vulnerabilities upon which to build an effective cybersecurity strategy.

5 DEVELOP CYBERSECURITY STRATEGY

GENERAL CONSIDERATIONS

Developing a strategy for cybersecurity, like any strategic planning, is based on an understanding of the goals and objectives of the process, an awareness of environmental factors, internal capabilities and limitations, and the formation of an actionable and measurable plan to advance from current state to the desired end state. It is a discipline, the value of which is only partially measured in the final product.

Of great benefit is the engagement of a broad, interdisciplinary team in the process of developing the strategy. During this effort, the executive management team interacts with IT managers, the legal and finance teams, and leaders from the operational business units to develop a comprehensive approach. In doing so, the team has the opportunity to build trust, enhance culture (including a "security culture," to be discussed later), and build consensus on a common vision. When challenging times arise later- such as during a major breach or system crash- the strength of these ties will enable a faster and more coordinated response.

> *"Cybersecurity is very much the domain of the human resources manager… It's the domain of your marketing or development department… Therefore this is a classic enterprise risk. You need your whole business or organization to consider this risk from their point of view."*
> -Julia Graham, Chief Risk Officer, DLA Piper

It is also important to remember that the cybersecurity strategy is an integral part of the overall enterprise strategy (which includes business objectives, competitive positioning, non-cyber risk management and other elements). It should not be a separate endeavor. While the focus of this handbook is on managing the workforce for effective cybersecurity, a critical imperative to ensure alignment at the outset between business strategy and cybersecurity strategy.

TASK 1: DEVELOP GOALS AND OBJECTIVES

Developing a cybersecurity plan begins with understanding what the enterprise is trying to accomplish, which in turn is all about managing cyber risk. Like managing any other kind of risk, the goal is not 100% security, which is never possible. Rather, it is about understanding the particular risk tolerances of the enterprise. There are many factors to consider, including regulatory compliance (PCI, HIPAA and other industry-specific regulations), impact to customers, financial and operational impact of breaches, reputational risk and competitive position. At the outset, the degree of

acceptable risk must be established, as it will drive subsequent planning and investment decisions.

Some questions to address during this process include:

- What are specific standards which must be met in order to comply with applicable regulations?
- What are the legal and financial implications of non-compliance?
- What are the other drivers of risk tolerance that matter most to the enterprise?
- What are the possible impacts of a cyber attack beyond the enterprise itself-customers, suppliers, infrastructure, etc.?
- What big unknowns should be considered during the planning process?
- What constitutes acceptable risk?

TASK 2: ASSESS CAPABILITIES AND LIMITATIONS

Every organization has strengths and weaknesses, assets and liabilities, capabilities and limitations, which can be brought to bear in any effort, including cybersecurity. In order to develop a comprehensive and realistic strategy, the enterprise must account for these attributes. Here, too, there are many ways to conduct this phase of planning. At a minimum, the following questions should be answered:

- What are inherent strengths in the nature of the business, organizational structure, sourcing strategy, supply chain and other factors which will enhance the security of data and systems?
- What are inherent weaknesses in the nature of the business, organizational structure, sourcing strategy, supply chain and other factors which will diminish the security of data and systems?
- What technical capabilities can be leveraged (e.g., a software company will have coders on staff who can be deployed to address vulnerabilities)?
- What non-technical capabilities can also be leveraged (e.g. the endorsement of credible third parties during potential crises)?
- What areas show obvious lack of resources?

TASK 3: INTEGRATE KEY ELEMENTS OF STRATEGY

To be comprehensive, a cybersecurity plan must address risk through a multi-layered approach:

1. Prevention: Solutions, policies and procedures need to be identified to reduce the risk of attacks

2. Resolution: In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat
3. Restitution: Companies need to be prepared to address the repercussions of a security threat with their employees and customers to ensure that any loss of trust or business is minimal and short-lived

In order to provide these layers of security and resilience, the strategy must provide or enable specific capabilities:

Situational awareness- To support an awareness of infrastructure or information risk related to configuration or patching weaknesses, exposure, attacks, and deliberate or accidental misuse, through implementation of security monitoring technologies and operational monitoring of these technologies.

Continuous monitoring– The goal of continuous monitoring is to provide real-time awareness of enterprise security posture, enabling departments to address threats and to remediate vulnerabilities proactively before they can be exploited.

Data protection and management– As demonstrated in a succession of well publicized security events, the protection of privacy and other sensitive information is one of the most significant challenges faced in organizations today. This becomes even more challenging when addressed in the context of protecting access. Opening the information infrastructures to provide improved access to the right information for authorized users- anywhere, anytime, and any mission securely and reliably- is fundamental to an organization's ability to preserve and improve its mission capabilities.

Network centric– The network-centric approach focuses on providing defense at the periphery. This is what many would consider the traditional approach to providing security for an enterprise. While this method of protection is still valid, a more radical approach to security must include the life cycle of data, from creation, how it is used when valid, its use during any archival or retention requirements, and through its proper method of destruction.

Access control– In meeting the two significant objectives of protecting authorized users' access to the right information, the organization must first strengthen its ability to granularly establish and enforce access rules, and then tie these rules to its information assets so that only those individuals with rights to information have those rights. In addition, to address the access objective of reliability, the organization must deploy secure, reliable, capacious, and diverse access solutions that allow users access to needed information- anywhere and at any time.

An enterprise may choose to leverage the NIST Cybersecurity Framework as a guide for developing an overall strategy. Originally intended for critical infrastructure providers, the elements of this framework are broadly applicable:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Secuirty Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CCO	Communications

Figure 4- NIST Cybersecurity Framework Core

TASK 4: BUILD UPON CRITICAL CONTROLS

The NIST Cybersecurity Framework itself is mapped to the Critical Controls, and the Controls themselves provide a means to prioritize action- even within a broader strategy. Because of this, the Critical Controls can be the cybersecurity plan itself with little modification. For enterprises engaged in a detailed strategy process, the 20 Critical Controls themselves can be further assessed and integrated into the strategy in a more nuanced and detailed manner, including the implementation of specific sub-controls.

> *"If you're an enterprise out there and you don't know where to begin - begin with the Controls."*
> -Jane Lute, President & CEO, Council on CyberSecurity

Regardless of approach, a highly focused and direct starting point is provided in the "First Five Quick Wins[xii]": sub-controls that have the most immediate impact on preventing attacks. These actions are specially noted in the Critical Controls publication, and consist of:

1. Application whitelisting (found in Critical Control 2);
2. Use of standard, secure system configurations (found in Critical Control 3);
3. Patch application software within 48 hours (found in Critical Control 4);
4. Patch system software within 48 hours (found in Critical Control 4); and
5. Reduced number of users with administrative privileges (found in Critical Controls 3 and 12)

What matters most here is that the enterprise has a coherent plan in place- meaning a common approach, in which everyone understands their roles and responsibilities, and which can be measured to ensure progress. Without a sound and measurable cybersecurity strategy, workforce planning becomes an isolated exercise without focus.

TASK 5: DEVELOP ACTION PLAN

No amount of time and effort spent on developing a plan will benefit the organization unless the plan is tied to a set of *specific* and *measurable* actions. The key components of the strategy must be broken down (much like a Work Breakdown Structure, per the Project Management Institute[xiii]) into specific tasks for specific individuals within specific timeframes. This means that any stated goal or objective must be accompanied with a means to actually *accomplish* it. Furthermore, these tasks must be measurable. In any enterprise, close attention is usually paid to performance metrics. Goals or tasks which are not measured, meanwhile, can easily become "nice-to-have" items that are set aside in the daily pressure to deliver on other metrics which are tracked by senior leaders.

> *"Accordingly, boards should put time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same industry."*
> -Luis Aguilar, Commissioner, Securities and Exchange Commission

There are many frameworks and templates for enterprise planning, each with their own benefits. The format matters much less than the content, and it must always be remembered that after a certain point in planning, there is diminishing return as additional time spent refining the plan takes away time from meaningful action.

6 LINK ROLES & CONTROLS

LINKAGE

In order to properly implement a comprehensive cybersecurity strategy, the workforce- the *entire* workforce, from CEO down to newest intern- must be aligned. Many of the activities in the plan will need to be conducted by IT professionals, some of whom may be designated as full-time security professionals. In turn, these professionals needs to have the right KSAs to implement the Critical Controls.

By mapping the roles in the NICE framework to the Critical Controls, we see how a workforce can be organized around key tasks associated with Critical Controls implementation. And these tasks, in turn, can be prioritized based on the Critical Controls themselves.

Mapping of the 31 specialty areas within the NICE framework (which correspond to common roles we find in the job market today) to the Critical Controls at the level of KSAs yields concentrations which indicate closer alignment between individual roles and specific Critical Controls. The KSAs, used here because they are the most discrete level of analysis in the NICE framework, have been associated with each Critical Control based on whether they are necessary for implementation of that Critical Control.

> *"A company must also have the appropriate personnel to carry out effective cyber-risk management and to provide regular reports to the board."*
> -Luis Aguilar, Commissioner, Securities and Exchange Commission

The heat map below shows the degree of concentration of aligned KSAs from each specialty area to each Critical Control, supported and supplemented by the input of SME's on the Council's Roles & Controls panel:

Degrees of Alignment

Lower 1 2 3 4 5 Higher

NICE Categories	NICE Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
		Critical Security Controls																			
Securely Provision	Information Assurance Compliance	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	2	2	2
	Software Assurance and Security Engineering	3	4	3	2	2	5	2	2	3	2	2	2	2	2	2	2	2	3	3	2
	Systems Security Architecture	5	5	4	3	3	4	5	5	4	5	4	5	4	3	4	5	5	3	4	4
	Technology Research and Development	2	2	3	2	1	3	3	2	2	2	2	3	2	3	3	2	3	3	2	3
	Systems Requirement and Planning	5	4	5	3	3	4	5	4	3	5	4	4	4	4	4	4	4	2	4	4
	Test and Evaluation	2	2	2	2	1	2	2	3	2	2	2	2	2	1	1	2	2	2	2	2
	Systems Development	5	5	4	3	2	4	4	4	4	4	4	5	3	3	4	5	5	3	2	4
Operate and Maintain	Data Administration	1	2	2	1	1	1	1	3	1	1	1	2	1	2	1	1	2	2	2	1
	Knowledge Management	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	2	1	1
	Customer Service Tech Support	2	2	2	2	2	1	2	2	1	2	2	2	2	2	2	3	2	2	2	2
	Network Services	4	2	3	2	3	1	5	2	2	5	4	3	4	3	3	2	4	2	3	3
	Systems Administration	3	3	3	2	2	1	3	2	2	3	3	2	2	2	3	2	1	2	2	2
	Systems Security Analysis	4	4	4	3	2	3	4	4	3	4	3	4	3	2	4	4	5	3	3	4
Protect and Defend	CND Analysis	4	4	4	4	5	3	5	3	3	5	4	4	5	4	4	2	3	3	4	4
	Incident Response	1	1	2	2	3	1	2	2	2	2	2	1	2	2	1	1	2	2	2	2
	CND Infrastructure Support	2	2	2	2	3	1	3	2	2	3	3	1	3	2	2	1	2	2	2	2
	Vulnerability Assess & Management	2	2	2	3	3	2	2	2	2	2	2	2	2	2	2	1	3	2	2	4
Investigate	Digital Forensics	2	2	2	3	4	3	2	3	3	2	2	3	3	2	2	2	2	3	2	2
	Investigation	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Collect & Operate	Collection Operations	5	4	4	5	3	3	4	3	4	4	4	2	4	4	3	4	4	4	3	3
	Cyber Operations Planning	3	3	3	4	3	3	4	4	4	3	3	3	4	4	2	3	2	3	2	3
	Cyber Operations	3	3	4	5	4	2	4	3	2	3	2	3	5	3	2	3	3	4	2	2
Analyze	Threat Analysis	4	4	4	4	5	5	4	3	3	3	4	3	5	4	2	4	4	4	5	5
	Exploitation Analysis	4	3	3	4	4	4	4	3	3	4	3	2	4	3	2	3	3	4	3	4
	All Source Intelligence	3	3	3	3	5	3	3	3	2	3	3	3	4	4	2	2	3	3	3	4
	Targets	2	3	3	3	4	2	3	2	2	3	1	1	3	3	2	2	2	4	3	4
Oversight and Development	Legal Advice and Advocacy	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1
	Strategic Plan & Policy Dev	1	1	2	2	1	2	2	2	2	1	1	2	2	1	1	1	1	2	1	2
	Education & Training	2	1	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	1	2
	Info Sys Sec Ops (ISSO)	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	1	3	3	2	2
	Sec Program Mgmt (CISO)	3	3	3	2	2	2	3	3	3	3	3	3	3	3	3	2	3	3	2	3

Figure 5- Mapping of NICE Specialty Areas to Critical Security Controls

GENERAL OBSERVATIONS

A review of the heat map above yields some broad observations, which can assist in workforce planning:

- As the category totals show, the majority of Critical Controls can be significantly addressed by implementing the NICE specialty areas in the Securely Provision and Operate & Maintain categories. An obvious exception to this is Critical Control #5 (Malware Defenses), which appears to be most frequently addressed by the specialty areas in the Protect & Defend category.

- The five specialty areas that on average address the most KSAs, in order of degree, are:
    - 22%- Systems Security Architecture (Securely Provision)
    - 21%- Systems Requirement and Planning (Securely Provision)
    - 21%- Systems Development (Securely Provision)
    - 20%- CND Analysis (Protect and Defend)
    - 18%- Systems Security Analysis (Operate and Maintain)
- The specialty areas in Securely Provision have a greater tendency to address the KSAs for many Critical Controls, with the largest amount of KSA overlap of any category. With a high concentration of generic, redundant KSAs, this overlap may be cause to consider collapsing or consolidating a few of these roles. For enterprise workforce planning, this suggests the *opportunity to leverage a smaller number of roles to implement a larger set of Critical Controls.*

TIP: Filling roles within Securely Provision will help implement the largest number of Critical Controls

- The specialty areas in the Operate and Maintain category have less overlap, but as a whole, this category addresses the largest percentage of KSAs, accounting for 60% of the total. This suggests that each specialty area is unique in addressing specific Critical Controls.
- Not surprisingly, Critical Control 6 (Software Application Security) shows a high degree of alignment with Software Security and Engineering. This high correlation appears to be an outlier for both the Critical Control and specialty area. This is also a reflection of the unique function of this role.

While not an exhaustive analysis, the mapping serves to highlight key roles that are particularly relevant to implementing the Controls. Additional analysis of this linkage, provided for each of the Top 20 Critical Security Controls, is available in Appendix C.

FIRST FIVE QUICK WINS

As noted previously, there is a subset of Critical Controls which provide the most immediate and greatest benefit. Based on the analysis provided in Appendix C, we can see which roles should be at the top of the list for sourcing, deployment and management, as they are necessary for properly implementing the First Five Quick Wins.

- Application whitelisting (found in Critical Control 2)
    - Information Assurance Architect, Information Security Architect
    - Information Assurance Developer, Information Assurance Engineer

    - Information Systems Security Manager, Information Assurance Operational Engineer, Information Security Specialist
- Use of standard, secure system configurations (found in Critical Control 3)
    - Business Process Analyst, Computer Systems Analyst, Requirements Analyst
    - Information Assurance Architect, Information Security Architect
    - Computer Network Defense Analyst, Incident Analyst, Network Defense Technician
- Patch application software within 48 hours (found in Critical Control 4)
    - Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician
    - Business Process Analyst, Computer Systems Analyst, Requirements Analyst, Human Factors Engineer
    - Information Systems Security Manager, Information Assurance Operational Engineer, Information Security Specialist
- Patch system software within 48 hours (found in Critical Control 4)
    - Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician
    - Business Process Analyst, Computer Systems Analyst, Requirements Analyst, Human Factors Engineer
    - Information Systems Security Manager, Information Assurance Operational Engineer, Information Security Specialist
- Reduced number of users with administrative privileges (found in Critical Controls 3 and 12)
    - Information Assurance (IA) Architect, Information Systems Security Engineer
    - Business Process Analyst, Computer Systems Analyst
    - Computer Network Defense Analyst, Incident Analyst, Network Defense Technician

What matters here is that the First Five Quick Wins are addressed by the specialty areas represented by these roles. In other words, the job titles here are a sampling of job titles commonly associated with implementing the Critical Controls which comprise the First Five Quick Wins.

LINKAGE TO THREAT VECTORS

In addition to the linkage of roles to First Five Quick Wins, the common basis of Critical Controls provides a natural linkage of roles to major threat vectors identified by

various threat reports. Breach reports are published on an annual basis by the cybersecurity vendor community. These reports identify the most vulnerable areas across enterprises that were breached in the previous year. How can organizations make the best use of such reports when it comes to ensuring they have the right resources on staff to address these high risk areas?

Applying the Critical Controls to the annual reports yields the steps necessary to identify and eliminate the most common attacks that impact organizations. Taking the recommended Critical Controls and applying them to the NICE framework then reveals the key job areas and tasks that are needed to carry out the actions necessary to increase the organization's security posture.

BREACH REPORTS	CRITICAL SECURITY CONTROLS	NICE FRAMEWORK CATEGORIES
Verizon DBIR	5, 12, 13	Securely Provision/Operate and Maintain
HP	3, 6, 10	Securely Provision/Operate and Maintain
FireEye	3, 5, 6	Securely Provision/Operate and Maintain
Symantec	3, 5, 7	Securely Provision/Operate and Maintain

Figure 6- Threat Reports Linked to Controls Linked to NICE Framework

In short, the mapping of NICE framework-based roles to Critical Controls provides the linkage of workforce planning to enterprise cybersecurity planning. Based on this mapping, specific roles have been identified for implementation of each Critical Control (Appendix C). In turn, the broader workforce plan can be developed.

7 DEFINE WORKFORCE REQUIREMENTS

ALIGNING THE WORKFORCE TO CYBERSECURITY STRATEGY

It is no exaggeration to say that even in the highly-technical work of IT operations and cybersecurity, people are the most important factor. No enterprise can be secure without the right people, in the right places, with the right skills and empowered with the right authorities and supporting resources.

But defining cybersecurity workforce requirements can be a difficult task, especially for those who are not familiar with what IT operations and security professionals do on a daily basis. Furthermore, it's often not very clear who is supposed to be doing what- traditional IT operations perform some essential security tasks for the enterprise, while there specific and highly-focused tasks performed by cybersecurity professionals.

In this section, you will find the essential tasks which everyone in the enterprise needs to be doing, as well as the tasks which IT operations and mission-critical cybersecurity professionals must focus on.

TASK 1: ASSIGN CYBERSECURITY TASKS ACROSS ENTIRE WORKFORCE

While it is often tempting to view cybersecurity as primarily a technological challenge, and thus relegated to the work of IT and security professionals, the problem is more like public health or public safety, where the actions of everyone affect the health and safety of everyone. In the modern enterprise, no degree of technical sophistication can remove all of the vulnerabilities inherent in the workforce itself, including social engineering (such as emails with malicious links), poor credential management (such as weak or unprotected passwords), and use of insecure or poorly-configured devices and applications (such as connecting "dirty" thumb drives or installing applications from unverified websites). In order to properly secure the enterprise, the workforce itself must be "secured." Fortunately, many of the tasks associated with this effort are not onerous- rather, there are some basic practices that every employee should exercise to ensure good cyber hygiene.

The following Essential Tasks Pyramid highlights the tasks that must be performed by everyone in the enterprise, with additional tasks assigned to those with increased responsibility for data and systems. Higher levels of the pyramid indicate tasks which are above and beyond those already performed in lower levels. As employees are assigned greater control over enterprise data and systems, the number of essential tasks increases.

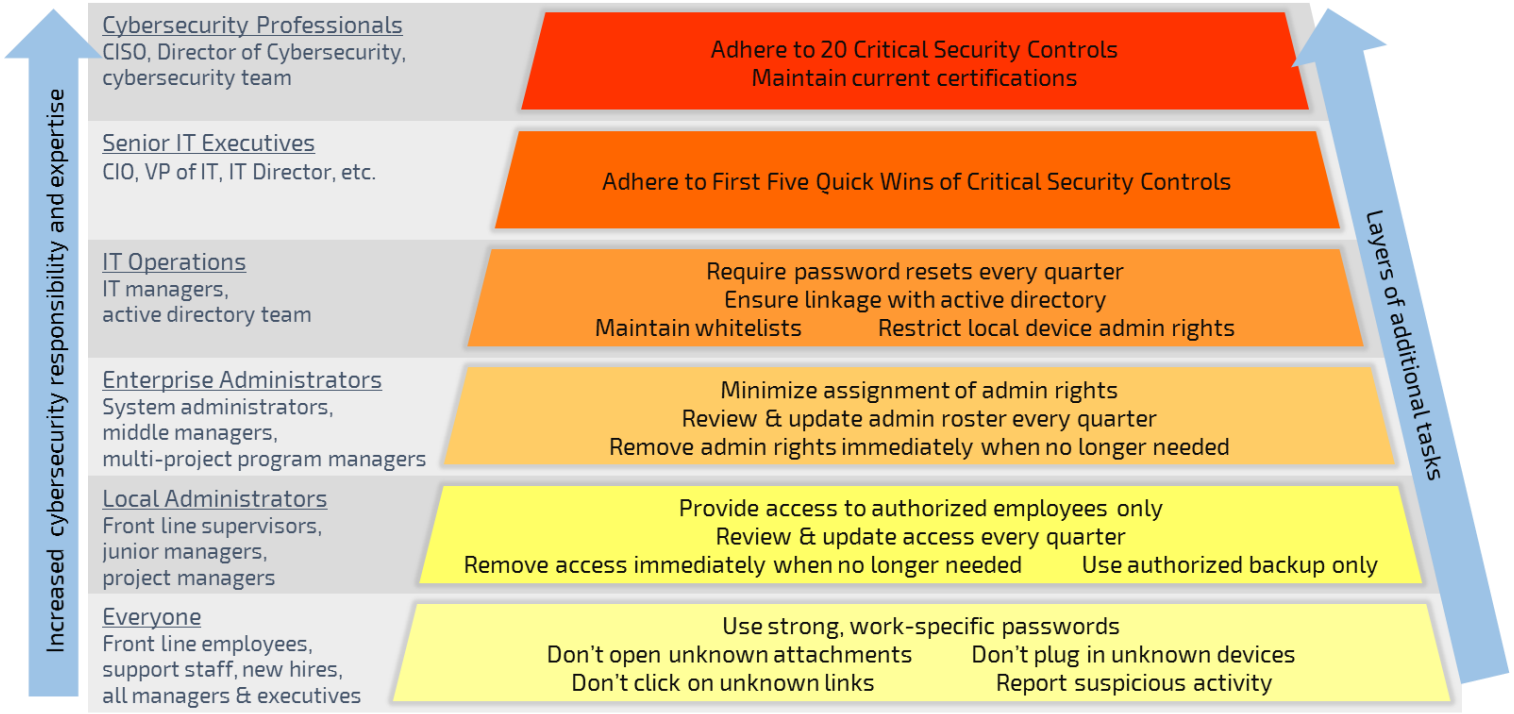


Figure 7- Essential Tasks Pyramid

For example, a front line supervisor may have administrative rights on a site within an online collaboration tool (such as SharePoint), which means that the supervisor has greater responsibility over enterprise data (the content of the site) and systems (access privileges to the site), than an individual contributor on the team. Because of this, the supervisor must perform essential tasks on the second level of the pyramid, such as reviewing access on a quarterly basis, which are above and beyond those already being performed according to the first level of the pyramid.

This graphic serves as a quick reference guide; more information is available on the Council's website (http://www.counciloncybersecurity.org/workforce/).

TASK 2: ALIGN IT OPERATIONS WITH SECURITY FUNCTIONS

As indicated on the Essential Tasks Pyramid, many functions beyond the essential hygiene tasks assigned to everyone are assigned to those who have more hands-on interaction with enterprise data and systems. These functions usually fall into one of two groups of people: IT operations and cybersecurity. While interrelated, corporate IT and security functions are not necessary the same, and can often operate at cross purposes, given different priorities.

IT operations include Internet access, email and other communications tools, business productivity tools, including hardware, software, databases, and supply chain dependencies, and the corporate network. IT departments are responsible for granting access to systems and distributing or collecting devices. For these

professionals, availability and reliability often trump any other priority- including security.

Meanwhile, a typically much smaller cybersecurity team is responsible for securing the information that encompasses corporate, partner, and customer data, across all networks, devices, software, and hardware. For them, security and integrity are paramount. Both functional areas are critical to ensuring a strong security posture for the enterprise- the challenge is to harmonize their activities.

To do this, it's important to understand the different functions, and potential conflicts between IT and security, as outlined below:

FUNCTIONAL AREAS	IT OPERATIONS	CYBERSECURITY
Email & communications	Automated sign-on, few restrictions on attachments, multi-device access	Strong authentication (difficult passwords, changed frequently), limits on attachments, spam filtering
Collaboration tools	Automated sign-on, ease of sharing, ease of adding new members	Strong authentication, limits on file downloads, approval gates for adding new members
Website	Rich content, easy to download files, easy to update	Careful coding, approval gates for modifications
Databases	Connected to other databases, ease of access, easy to modify content	Limited access, limited administrative privileges
Mobile access	Ease of access, connected to enterprise applications	Strong authentication, compartmentalization of corporate data, remote wipe capability

Figure 8- Competing Priorities of IT Operations and Cybersecurity

Many enterprises, especially small and medium-sized companies, do not have any designated cybersecurity professional. And in many enterprises, the security roles are incorporated into traditional IT roles. It is critical that one person is designated, in writing, as the individual who has principle responsibility for cybersecurity, in order to ensure that proper policies and procedures are in place. This may be a part-time or full-time assignment, depending on the scope and complexity of operations.

Regardless of who has final authority, it's important to address some key areas that are foundational. Whomever is responsible must develop policies and procedures, and implement them in the following areas:

1. Security awareness training
2. Encrypted data at rest and in motion
3. Use of firewalls
4. Intrusion prevention services
5. Web security monitoring, and reporting
6. Data loss prevention
7. Lock-down of desktops, laptops, and mobile devices
8. Use of strong passwords with forced changes every 60 days
9. Classification of public, private, and protected data
10. Separation of data and access based on content (critical data vs. noncritical)
11. Restricted access
12. Whitelisting of applications
13. Wireless network security
14. Mobile device management
15. Network monitoring tools
16. Vulnerability assessment

STEP 3: FOCUS CYBERSECURITY PROFESSIONALS ON PRIORITY TASKS

While good cyber hygiene- individually and collectively- is an essential element of enterprise security, a defining characteristic of well-secured enterprises is the involvement of highly capable, technically sophisticated cybersecurity professionals who possess the right mix of knowledge, skills and abilities to identify, protect, detect, respond and recover from cyber attacks. There is a tremendous need for, and painful shortage of, professionals who can bring to bear hands-on skills to counter the sophisticated and ever-evolving threats presented by other highly-capable and technically sophisticated, but nefarious, actors around the world. Despite double digit annual growth of the

> *"Attempts to professionalize a cybersecurity occupation should only be undertaken when the field is" well-defined" with "stable knowledge and skill requirements," and that there is credible evidence of skill deficiencies in the workforce."*
> –Professionalizing Cybersecurity: A Path to Universal Standards and Status

workforce in recent years, shortages remain[xiv]. An effective workforce plan, in support of a sound cybersecurity strategy, requires a balance of well-rounded IT operators and sophisticated cybersecurity professionals who can successfully tackle the most complex challenges.

As noted above, many of the roles which are essential to implementing Critical Controls are those which perform functions related to architecture, resource planning and security analysis. These reflect a breadth of coverage, based on the KSAs which are necessary for Critical Controls implementation. They are foundational to any workforce plan, and must be properly sourced in order to ensure coverage of essential KSAs.

> *"There needs to be a professional cybersecurity workforce… capable of inculcating standard best practices into standard professional bodies of knowledge thereby enhancing the efficiency and effectiveness of cybersecurity technologies and strategies."*
> -Professionalizing Cybersecurity: A Path to Universal Standards and Status

However, there are some specific roles which are mission-critical because of high criticality to enterprise security *and* high degree of technical sophistication. These roles merit special consideration in workforce planning, as they require careful selection and investment to ensure ongoing training, development, and retention. As noted in a 2012 report by the Cyber Skills Task Force[xv] of the Homeland Security Advisory Committee convened by the Secretary of Homeland Security, and supported by the 2014 paper by the Council on CyberSecurity[xvi], the following are the ten roles which meet this criteria:

- System and Network Penetration Tester
- Application Penetration Tester
- Security Monitoring and Event Analyst
- Incident Responder In-Depth
- Counter-Intelligence/Insider Threat Analyst
- Risk Assessment Engineer
- Secure Coder and Code Reviewer
- Security Engineer/Architecture and Design
- Security Engineer/Operations
- Advanced Forensics Analysis

Emphasis on proper selection and management of mission critical roles will elevate the competence of the broader workforce. Because of the technical sophistication of these professionals, they are more likely to identify new threats, attack vectors and

vulnerabilities, while discovering creative new ways to defeat them. At the same time, they serve as mentors to junior professionals, while providing a career path of progressively challenging and rewarding roles. So there are long-term benefits beyond the immediate functions performed by mission critical roles which make them particularly valuable to the enterprise.

These roles should not take precedence over those identified through the mapping of roles to Critical Controls (in Chapter 6), since implementation of the Critical Controls must remain the priority. But an appreciation for the benefit of having these technically sophisticated professionals on the team should inform workforce planning in advanced stages- perhaps after the First Five Quick Wins are properly supported.

CERTIFICATIONS

One of the greatest challenges in managing the cybersecurity workforce today is a lack of clarity and consistency among the many professional certifications which exist in the market. Cybersecurity remains a profession that has not yet matured to the degree of many others, such as medicine, law and accounting, which have common bodies of knowledge, consistent standards of due care, a recognized authority on professional standards, mechanisms for enforcing professional standards, consistent training and education guidelines and consistent career pathways. As noted by Francesca Spidalieri and Sean Kern in "Professionalizing Cybersecurity: A path to universal standards and status"[xvii], there are many advantages to increased professionalization and potential avenues to realize a better state for the community overall.

However, the workforce remains very fragmented. For those who must hire and manage these professionals, it can be difficult to assess an individual's degree of competence necessary to successfully perform in any given role. One way is to look for certifications. The following is a non-exhaustive list of the major certification providers:

- Global Information Assurance Certification (GIAC), www.giac.org
- International Information Systems Security Certification Consortium $(ISC)^2$, www.isc2.org
- CompTIA, www.comptia.org
- EC Council, www.eccouncil.org
- Information Systems Audit and Control Association (ISACA), www.isaca.org

These certifications vary greatly in their degrees of specificity for each role. Some reflect broad understanding of general concepts and practices, while others emphasize specific knowledge in certain domains. Some reflect knowledge, while others test for hands-on skills. While there is no definitive way to ensure that a

certification provides every attribute necessary for successful performance in a role, there is some degree of alignment which can be drawn. The following is a sampling of certifications which support some of the mission-critical roles:

MISSION CRITICAL FUNCTIONS	COMPTIA	SANS- GIAC	(ISC)²	EC-Council	ISACA
System and Network Penetration Tester	CASP Advanced Security Practitioner	GPEN GPXN Exploit Researcher and Advanced Penetration Tester		LPT Licensed Penetration Tester	
Application Penetration Tester	Mobile App Security+	GWAPT Web Application Penetration Tester	CSSLP Secure Software Lifecycle Professional		
Security Monitoring and Event Analyst		GSNA Systems and Network Auditor		ECIH Network Handler	CISA Information Systems Auditor
Incident Responder In-Depth		GCIH Certified Incident Handler			
Counter-Intelligence/Insider Threat Analyst		GXPN Exploit Researcher and Advanced Penetration Tester		ECSA Security Analyst	
Risk Assessment Engineer	CASP Advanced Security Practitioner	GCIA Certified Intrusion Analyst	CAP Authorization Professional		CRISC Risk and Information Systems Control
Secure Coder and Code Reviewer		GSSP Secure Software Programmer		ECSP Secure Programmer	

Security Engineer/Architecture and Design	Security+ Mobility+ Cloud+	GCWN Windows Security Administrator	CISSP Information Security Systems Professional		CISM Information Security Manager
Security Engineer/Operations	Security+ Server-	GCFW Firewall Analyst			
Advanced Forensics Analyst		GCFA Forensics Analyst	CCFP Cyber Forensics Professional	CHFI Forensics Investigator	

Figure 9- Alignment of Select Certifications with Mission Critical Roles

COMPETITIONS

One of the best ways to identify talent is through hands-on competitions. Recognizing that cybersecurity talent is not always found in traditional academic settings, these competitions identify, assess, train and develop aspiring professionals. By emphasizing hands-on skills in qualifying online competitions, in-person training exercises and capture-the-flag contests, often in summer camp-style settings, the competitions are able to tap into a broader base of talent, while providing prospective employers with a sense of real skill levels.

The Council is home to U.S. Cyber Challenge (www.uscyberchallenge.org), or USCC, which leverages an online gaming environment (CyberQuest) to qualify prospective camp attendees, who are then invited to a week-long in-person camp held at a partner university. There, campers receive formal instruction in topics which range from web application security to mobile devices, participate in ethics panel discussions, attend a job fair and compete for scholarships in a capture-the-flag event. USCC is also a research and development program to refine the means through which talent is identified, assessed and tracked. By tapping into programs like USCC, employers are able to access vetted talent in a different, and arguably much more effective way, than through the usual process of resume scans and interviews.

CONSIDERATIONS FOR HIRING NEW TALENT

There is unfortunately no simple solution to the challenge of finding capable cybersecurity professionals, as there is not one single profile (with specific education, training, experience, certifications, and competitions) which definitively covers all KSAs necessary for each role. The cybersecurity profession will continue to evolve, but for now workforce planners and hiring managers must sort through the existing assortment of certifications to find the ones most relevant to enterprise needs.

In order to ensure the best possible outcome in hiring a cybersecurity professional, the following considerations should be given:

- Become familiar with the major providers and what they offer in terms of specificity and hands-on skills assessment
- Identify the certifications most relevant to each role
- Heavily weight hands-on experience, regardless of certifications
- Heavily weight performance in cybersecurity competitions
- Consider formal training and education as indicators of interest, commitment and general understanding

8 OUTLINE SOURCING PLAN

GENERAL CONSIDERATIONS

Once the workforce requirements are understood, the enterprise must have a plan for how to source these roles. This process includes both *outsourcing*, in which external parties are the providers, and *insourcing*, in which necessary goods and services are deliberately purchased or hired within the organization. In deploying the cybersecurity workforce, each enterprise must determine which roles are better filled by their own employees or hired on, and which will be provided by external parties (such security service providers).

Outsourcing is a common business practice across a broad range of functions. In many cases, outsourcing IT provides benefits which include lower costs, additional expertise, operational efficiencies and lower burden on management.

> *"When it works, outsourcing offers companies compelling strategic and financial advantages,"*
> -Booz|Allen|Hamilton. Profits or Perils? The Bottom line of Outsourcing

For all of its advantages, however, outsourcing does not relieve an organization of its responsibility to secure data and protect systems, especially where regulatory compliance is an issue. Although an IT provider may have the ability to deliver an IT infrastructure of sufficient size and availability, this does not mean that the provider has the capability to fully understand the company's unique needs and requirements, including critical information assets and regulatory requirements. By articulating the knowledge, skills, and abilities associated with key IT security functions, enterprises can clearly articulate workforce requirements for outsourced IT, before contracts are signed and- more importantly- before problems arise.

For many large enterprises and federal government agencies, the primary drivers for sourcing are expertise and organizational flexibility. For small to medium businesses, outsourcing is often an unavoidable reality, especially for those whose core business is not closely linked to technology. Outsourcing makes it possible for smaller enterprises to enjoy many of the same capabilities as larger ones, but with more predictable- and generally lower- cost than building the capability internally.

> *"One caveat of outsourcing is that you can outsource business functions, but you cannot outsource the risk and responsibility to a third party."*
> -Verizon 2012 Data Breach Investigations Report

SOURCING STRATEGY

Sourcing strategy, particularly for the workforce, is not a one-dimensional exercise. To make any outsourcing decision, an enterprise must first have a reliable inventory of the types of data it collects, a value assessment of that information, and a knowledge of where it is stored. This can be surprisingly difficult, especially if IT management has been done on an ad-hoc basis, or as an ancillary duty within the business. Without this understanding of the type, business value and location of the information an organization possesses, it is impossible to establish outsourcing requirements. Although outside consultants may be able to assist in this inventory process (itself an outsourcing activity), maintaining the inventory, and ensuring it is used to inform IT outsourcing decisions should in most cases remain the responsibility of a trusted employee.

Certain types of data containing payment card information, health information, or other types of very sensitive information may be subject to additional regulation. Not all IT providers are willing or able to comply with the requirements of maintaining this type of data, nor is the burden of ensuring compliance fully transferrable to the provider. Ultimately, compliance will be the organization's responsibility, so it is imperative that not only information storage and processing requirements are clearly articulated, but that the outsourced provider's employees have the necessary KSAs to ensure compliance.

WHAT TO LOOK FOR

In order for IT outsourcing to be fully successful, both parties must agree in writing to the types of data which will be handled and how it will be secured. It is also critical that the limits of the provider's liability be clearly defined. For example the contract and supporting documentation could include a detailed agreement articulating the "roles and controls" necessary, as well as an accounting of what role or Critical Control is to be implemented by each party. The contract could also include a commitment to maintain the skillsets of each role involved. If an IT provider cannot produce a plan to train and retain employees with the requisite KSAs, it is unlikely the project can succeed.

The outsourcing agreement must describe how the security of data will be monitored and audited, including how potential indicators of breach or noncompliance will be communicated to the management. This mechanism for communication should also be tailored to fit into the crisis management and business continuity plans, as gaps between these two constructs can lead to extremely damaging incidents, such as the

breach which compromised the payment card systems of Target in late 2013[xviii]. This also suggests another requirement for outsourced IT, namely that the people who serve as the interface between the enterprise and the outsourced IT provider must have the requisite KSAs to understand the severity of a breach, the implications to the business, and any legal disclosure requirements.

The following are considerations for outsourcing various IT components:

IT COMPONENT	CONSIDERATIONS
Website Development	• What is the track record of the products made by the provider? Have any of its past websites/products been hacked. Will it still has access to the logs/architecture of the website? • Ensure that security is built into the development of the website. Are there backdoors, vulnerable code, etc. Ensure that code reviews and web app pentests are performed by a reputable third party prior to accepting delivery of the code. Ensure the code is properly commented and identify in the contract how sustainment of the code and bug fixes are handled.
Data Services	• Measures available to secure the input and output of the data -behind legacy security products-; presence or not of a tool for data theft analytics. • Validate the service provider has the adequate resources to fulfill their obligation
Enterprise Application Services	• Inquire about the security assurance level and cyber readiness assessment level of the service provider. • Validate the service provider has the adequate resources to fulfill their obligation. Ensure you know who is responsible for what….roles and responsibilities…exercise/test them.
Help Desk Services	• Inquire about the security assurance level and cyber readiness assessment level of the service provider. • Ways to audit/track violations or system admin access, access to employees or violations of privacy.
Infrastructure Management Services	• Inquire about the security assurance level and cyber readiness assessment level of the service provider. • Validate the service provider has the adequate resources to fulfill their obligation. Exercise continuity plans, fail over, disaster recovery, verify physical redundancy, etc.
Financial Transactions Services	• Understand data configuration and recovery system. Degree of segmentation of the network and access level based on "the need to know" • Validate/audit/track the accuracy and timeliness of transactions.
Payroll Services	• Understand data configuration and recovery system. Degree of segmentation of the network and access level based on "the need to know". • Validate/audit/track the accuracy and timeliness of transactions.
Human Resources Functions	• Understand data configuration and recovery system. Degree of segmentation of the network and access level based on "the need to know". • Adequately protect PII; encryption, NDAs, audit system accesses, etc.

Figure 10-IT Outsourcing Consideration

MANAGING THE OUTSOURCING RELATIONSHIP

As alluded to in the previous sections, management of an IT outsourcing project itself includes specific tasks, which may be spread across multiple individuals. These include maintaining an awareness of regulatory and legal compliance issues, understanding the changing business needs of the enterprise, sustaining effective liaison with the provider, and managing a smooth transition to and from outsourced IT systems.

Outsourcing agreements should be periodically reevaluated to ensure compliance with changing legal and regulatory frameworks. The person or persons who perform this task must be able to keep abreast of both the evolving data inventory of the business and changes to laws and regulations. They must also be able to translate those changes into contract modifications, as necessary.

As business needs change, someone must also have the ability to understand those changes and adjust the outsourcing agreement to ensure the enterprise is neither spending too much or too little for the services being outsourced. This requires a deep understanding of the core business, as well as a current understanding of the offerings of various providers.

Successful liaison between the IT provider and the enterprise requires a broad understanding of the business, the regulatory environment, the various types of incidents which may arise, and the policies and procedures for handling significant incidents.

TIP: The liaison role must be a solid cyber and business generalist, as well as an internal policy experts with access to appropriate decision makers

As the business grows and changes, multiple migrations to and from various outsourced IT systems may become necessary. Each transition requires someone with a good understanding of business continuity, a broad, general understanding of IT, and an acute attention to detail. These employees must make certain that primary business functions are not negatively impacted by the transition, that old systems are decommissioned fully, and that duplicate data is destroyed once it is no longer needed. A failure to perform this function adequately increases the attack surface of an organization significantly. For example, failing to decommission an old version of a front-end web application server might create an alternate, less secure path for intrusion into a back-end database with critical business information.

9 DEPLOY THE WORKFORCE

DEPLOYING SCARCE RESOURCES FOR MAXIMUM IMPACT

While it is imperative to define workforce requirements and determine the appropriate sourcing strategy for essential functions, the deployment of these roles within the enterprise is critical. A successful workforce plan- as defined by greatest positive impact to enterprise cybersecurity- is a function of *where* and *how* these essential roles are placed. In turn, this means the proper organizational placement of specific roles, and the enabling of these roles with proper reporting chains, responsibilities and authorities.

MANPOWER MAP

Given the countless organizational structures that exist across enterprises of vastly different sizes and widely different industry sectors, there is no simple, ready-made answer to where roles should be placed. However, there are guiding principles which provide criteria for how these decisions can be made in the most effective way possible. As displayed on the Manpower Map below, an intersection of the most salient attributes provides a sense of relative placement within the enterprise.

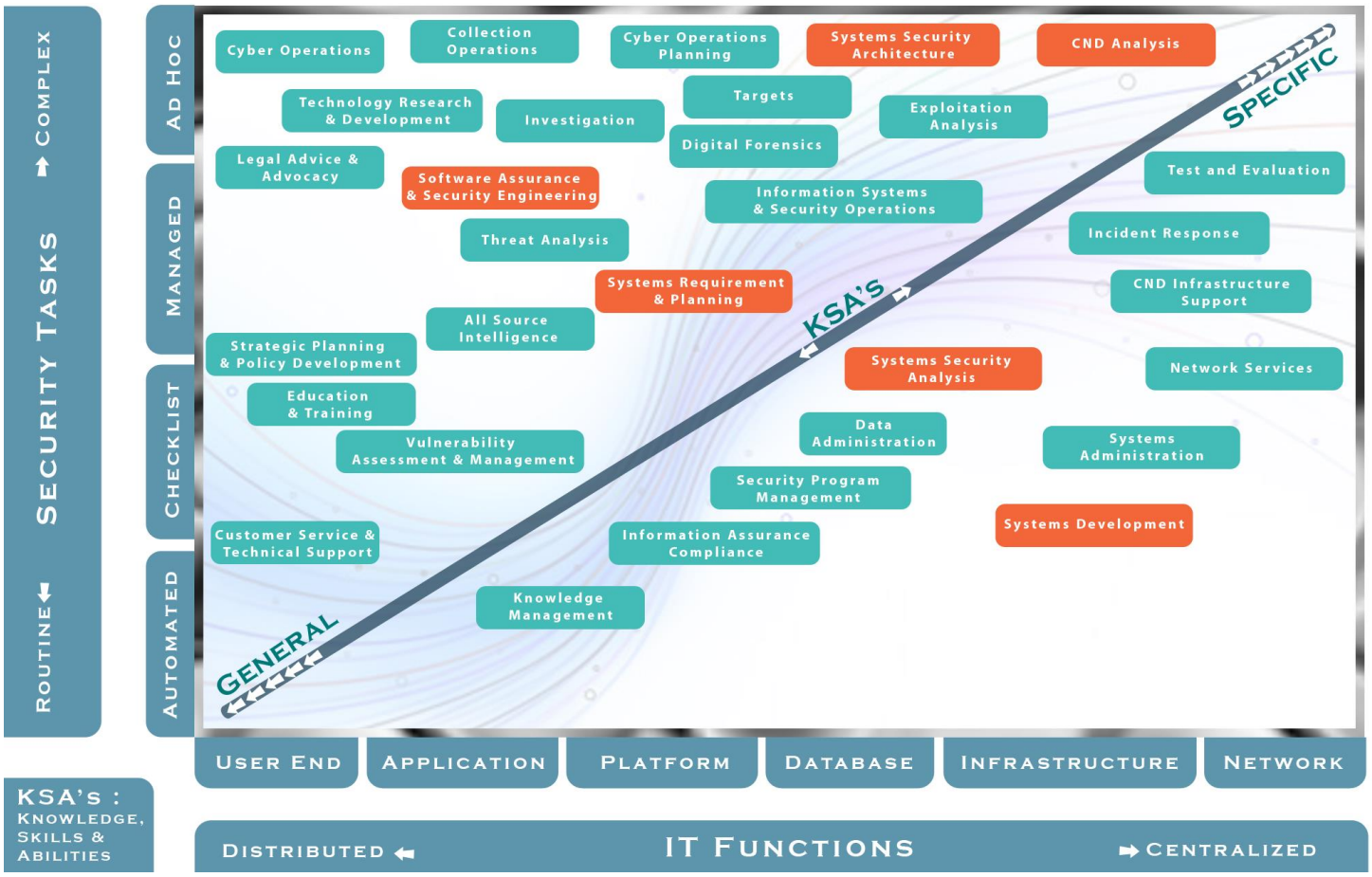


Figure 11 - Manpower Map for Enterprise Deployment

The roles plotted in the Manpower Map are the 31 Specialty Areas of the NICE Framework, representing all functions within cybersecurity in general. This mapping represents a distribution of the roles across two axes, representing different attributes:

1. Centrality of IT functions- this is a reflection of the primary functional area of the role relative to components of a typical enterprise IT environment, ranging from the most distributed functions supporting end users to the most centralized functions managing corporate networks and infrastructure ("IT Functions" or X axis)
2. Complexity of security tasks involved for that role- this is a reflection of the nature of security tasks involved, ranging from routine tasks which can be automated to the most ad hoc tasks requiring high-order technical sophistication and creativity ("Security Tasks" or Y axis)

The intersection of these two attributes yields a third dimension: the degree of specificity of KSAs, which means how technically-focused the role tends to be. The

plotting of each role provides a relative sense of the deployment of roles within the organizational structure. The highlighted roles are those with the strongest linkage to implementing the First Five Quick Wins.

Based on these features, the Manpower Map can be used to guide workforce deployment in the following ways:

- Placement- Decisions for where a role should be, both within an IT organization and relative to the broader organization, can be guided by relative position along "IT Functions" (X axis). For example, Education & Training or Knowledge Management roles may or may not be within the IT organization (likely not), but the mapping suggests that they must have easy access to, and be easily accessible by, end users throughout the enterprise. Meanwhile, Test & Evaluation roles, including the mission critical penetration testers, need to be close to the corporate center and do not need as much direct interface with end users, regardless of how they are sourced.
- Prioritization- Decisions for which roles to prioritize can be guided by relative position along "Security Tasks" (Y axis), since more routine tasks can be addressed through increased automation, less technically-proficient security staff, assignment of tasks to IT operations roles, or some combination thereof. Furthermore, prioritization can (and should) reflect the intersection of "IT Functions" and "Security Tasks," so that the roles appearing in the upper right part of the Manpower Map would naturally be prioritized over those in the lower left. Finally, the highlighting of roles most closely linked to the First Five Quick Wins provides a solid base for selecting the roles to emphasize.
- Authorities- Decisions for the degree of authority and latitude given to each role can be guided by the relative position of that role. While routine tasks, by their definition, require little modification, the more complex the tasks are the more nuanced judgment is required. Therefore, the roles higher on the vertical axis need more authority and latitude to successfully perform their duties. A consideration of the IT functions of each role can also provide a useful reference for determining authorities. In turn, these factors can help establish reporting chains, since roles with greater authorities and more latitude will, in most cases, require more seniority or the support of more senior managers.
- Training & Development- Ongoing support of professional development is necessary to keep the cybersecurity workforce current, and can also impact retention. At the same time, limited funding forces prioritization. By referencing the Manpower Map, prioritization of funding for training and development can be made, based on the relative position of the role and the specificity of the KSAs required to perform those functions.

As organizations mature, and as the broader cybersecurity workforce becomes more professionalized, some of these guidelines will become more specific. In the

meantime, the Manpower Map serves as a general reference for workforce planning and, more specifically, the deployment of the workforce within the enterprise.

OPTIMIZING THE WORKFORCE

As with any workforce, the performance and productivity of the team depends on many factors, including leadership (discussed in Chapter 10). Providing an environment in which cybersecurity professionals, as well as IT operations and all employees performing cybersecurity tasks, can thrive, the enterprise must implement HR policies designed to enable their success.

Key attributes of an optimized workforce include:

1. Multi-functional- The workforce must have individuals that are cross-trained in various cybersecurity functions; this provides opportunities for learning, mutual support, and reduced decision-making time when responding to crises
2. Constant learning- Resources and opportunities for learning and development enhance the performance of the workforce, encourage growth and often contribute to higher retention of top performers
3. Flexibility- The ability to work in a flexible, less-constrained environment supports creativity, innovation and higher job satisfaction

Effective workforce planning includes detailed forecasting of resource needs. Cybersecurity is changing so quickly that organizations can fail to plan for the necessary workforce or make poor hiring decisions, impeding the ability to implement effective security measures like the Critical Controls. Through proper deployment and efforts to optimize the workforce in an ongoing manner, the security posture of the enterprise as a whole can be improved and sustained.

10 MAINTAIN GOVERNANCE

GENERAL CONSIDERATIONS

No enterprise-wide priority can endure over time, or even be effectively implemented in the first place, without leadership attention. Protecting data, systems and infrastructure is no exception. As highlighted in a recent paper sponsored by the National Association of Corporate Directors[xix], cyber-related risks must be considered by boards of directors, and are increasingly discussed in earnest at that level. Furthermore, corporate culture is shaped primarily through the personal example of executive management- this includes building the right habits necessary for good cyber hygiene.

> *"Basic hygiene will prevent 80 to 90% of all known attacks."*
> -Jane Lute, President & CEO, Council on CyberSecurity

Even when a cybersecurity strategy has been developed, and a workforce plan drafted to support it, the job is not over. There is a need for ongoing governance of cybersecurity matters, including the workforce.

This includes three key aspects:

1. Emphasis- There must be ongoing emphasis on cybersecurity matters. This will build and reinforce a security culture (see below), while focusing management attention where and when necessary. Executive management must be involved in tracking performance against cybersecurity goals, and should provide the board with routine updates. More than anything else, this will continue to foster a cybersecurity mindset essential to success.
2. Involvement- Senior-level involvement is essential to making the necessary trade-offs involved in security decisions of any kind. There is no such thing as 100% security, since the enterprise must still perform important functions (a hospital must treat patients, an airline must fly passengers, and an electric utility must provide high-availability electric power). Critical decisions must be made to balance availability and reliability with integrity and confidentiality. Difficult choices must be made between investment in improving security and increasing efficiency. This is the realm of executive management, and cannot be ignored, lest by default the enterprise chooses the less secure option every time.

3. Leadership- The greatest asset of any organization is its people. Here the emphasis is not just on cybersecurity strategy and process, but on leading an effective workforce. If well led, carefully chosen, properly deployed, and enabled with the right authorities and tools, the cybersecurity workforce will repel threats, mitigate vulnerabilities and care for enterprise assets in new and creative ways which cannot always be foreseen or orchestrated at the top of the organizational structure. In this sense, effective management of the cybersecurity workforce becomes a broader enabler of success and should be viewed as such.

> *"There are two types of CEO, those that know their systems are being hacked – and those that don't. For pretty much any company I've come across, it should be one of the top three risks."*
> —Ian Livingston, former CEO, BT plc: World Economic Forum, Davos, January 2013

CULTURE OF SECURITY

Substantial progress can be made in protecting the enterprise by developing a culture of security[xx]. This comes down to awareness and attitude, which naturally lead to better action. And no factor is more significant to impacting awareness and attitude than leadership. Leadership- by example and emphasis- becomes the basis of a security culture in which the community of users contributes to the organization's overall security through a set of good practices at the individual level. Such an approach helps to mitigate some of the biggest risks to any organization, including cyber breaches through social engineering tactics like spear-phishing, and the risk created by increased adoption of bring-your-own-device (BYOD) policies.

> *"Cybersecurity issues often start with ordinary technology users who have not received proper training, do not take security seriously, or prize convenience over security by- consciously or not- sidestepping basic standards of best practices."*
> –Professionalizing Cybersecurity: A path to universal standards and status

An enterprise can begin to establish a culture of security by building an awareness of social engineering[xxi]. Social networks and forums are often used by cyber attackers to perpetrate targeted attacks on key resources and assets of the organization. A well-planned attack involves a phase of reconnaissance based on the relationship and habits of the targeted person(s) in order to craft phishing and spear-phishing emails with links that are more likely to be opened. In this arena, the end user is clearly the primary vulnerability- and the best defense.

Strong culture will increase the adoption of good cyber hygiene, including use of strong, work-specific passwords. More often, gaining access to one password, preferably the network administrator's one, allows the malicious actor to reach the overall organization's database, including the passwords database. (Recent breaches on a supposedly secure cloud platforms were due to exploiting multi-use passwords.[xxii]) A focused awareness and training program should be part of the hiring process for any new employee, and reinforced through annual refreshers for all employees.

TIP: Even sophisticated Advanced Persistent Threats (APTs) often make entry through entry points- like phishing emails!

BEST PRACTICES

The following is a brief list of suggestions for ongoing management of the cybersecurity workforce within a high-performance enterprise:

- Clear accountability- Along with a sound overall strategy, executive sponsorship is necessary to see the action plan through to completion. There must be one senior executive, within the C-suite, who is recognized as the leader who is accountable to the CEO and the board of directors for cybersecurity matters. This person can be the CIO, or another executive like the CFO or COO. Regardless, the person must have sufficient authority and influence to drive change.
- Establish a response team- Supporting the senior accountable leader, a Computer Incident Response Team (CIRT) should be formed. Standing by to execute response plans and coordinate enterprise activities, this is a cross-functional team representing all key functions from IT to finance, legal, communications and HR.
- Measure and report- As with any business initiative, no plan will be effectively implemented unless measured and reported. To this end, specific, measurable goals- per the cybersecurity strategy and associated workforce plan- must be aggregated in an intuitive manner for executive management review. One method is to turn the 20 Critical Controls themselves into a red/yellow/green dashboard[xxiii].
- Invest in training & development- The dynamic nature of cyber threats and the cybersecurity field require ongoing investment in the people who protect the enterprise. This ensures currency in tools, tactics and procedures, and is typically less costly than hiring a new employee. It also supports professional development, career progression and higher retention of top performers. Formal training and development can be provided by external certification providers, training centers, colleges and universities, or provided by in-house professionals.
- Build external relationships- Every enterprise is a part of a much broader network of partners, suppliers and customers. Furthermore, there are common threats and vulnerabilities faced by public and private entities across industry sectors, including national critical infrastructure. In order to foster collaboration and

- Coordination, relationships should be built with other entities, including law enforcement agencies who may need to be involved in future incidents.
- Develop career pathways- If the enterprise is large enough, various career pathways should be mapped out for cybersecurity professionals to provide development opportunities, incentives for performance and higher retention of top performers. These pathways should include roles in adjacent functions in IT operations and even other business functions, so that a rising senior professional is exposed to a broad cross-section of the enterprise.
- Establish mentorship- Professional development can be reinforced through a mentorship program which pairs senior leaders with junior professionals. This arrangement provides encouragement, support and guidance to the many aspiring cybersecurity professionals who may work for or support the enterprise. From a security perspective, a closer integration of cybersecurity professionals with senior leaders will also mitigate the insider threat problem, as greater loyalty can be fostered.
- Build the brand- Beyond the marketing value of a strong brand, the enterprise should seek to build a reputation as a company which emphasizes cybersecurity through implementation of the Critical Controls, developing a robust cybersecurity workforce and investing in the right tools and technologies. A strong security brand will be self-reinforcing, as top talent seeks to work for, or with, the enterprise.

In short, maintaining governance is an essential final element of the workforce management cycle. An emphasis on effective governance, and application of best practices for workforce management, will enable successful implementation of cybersecurity strategy, specific workforce plans and improve overall enterprise readiness and resilience against pervasive and persistent threats.

11 CONCLUSION

CHALLENGES

The effective management of a workforce oriented on improving enterprise cybersecurity is not an easy exercise, owing to many factors:

- Cybersecurity is a relatively new challenge; enterprises suffer from a lack of awareness or knowledge of what to do in the face of threats and vulnerabilities
- Security considerations often compete with other important drivers, such as availability, efficiency and cost
- Due to a pervasive "Fog of More," it is difficult to prioritize investment and action for maximum impact
- The cybersecurity field is not yet mature as a profession, lacking clarity and consistency of job definitions, competency models, education standards, certifications, career pathways and standards of care
- Cybersecurity functions and roles are varied- ranging from routine tasks expected of all employees to automated tasks managed by IT operations to highly technical and unique tasks performed by experienced cybersecurity professionals
- There is a lack of common reference frameworks to guide planning, support decision-making and provide necessary justification for changes and costs

These factors often conspire to push cybersecurity concerns- for their importance- out of the normal planning cycle and into the realm of afterthought or onto a list of "somebody else's problems." It is now abundantly clear that this approach is not going to work in a world of pervasive cyber threats and vulnerabilities.

RECOMMENDATIONS

While these challenges make cybersecurity workforce planning difficult, they are not insurmountable. There are tangible steps which all enterprises can take to integrate cybersecurity into enterprise strategy development, workforce planning, and ongoing governance. As outlined in this handbook, the following steps provide a cohesive approach to managing the workforce in a way that is aligned with cybersecurity best practice, while following the typical stages of workforce planning, deployment and ongoing management common to most enterprises:

1. Understand threats and vulnerabilities- First and foremost, an awareness of cyber-related risk must be developed. This includes foundational knowledge of basic IT and cybersecurity concepts, as well as an understanding of how

cybersecurity fits into overall enterprise risk management. This must be supplemented by more specific information pertaining to threats and vulnerabilities affecting a particular industry sector or even a single enterprise. Knowledge and understanding can be gained through publically-available resources, information sharing centers and vulnerability assessment tools for enterprise scanning.

2. Develop cybersecurity strategy- A cohesive enterprise strategy, which links business plans with risk management considerations including cybersecurity, is essential to cohesive enterprise action. Clearly stated goals and objectives, supported by an assessment of capabilities and limitations, must shape the strategy. The foundation for all cybersecurity action in an enterprise is provided by the Critical Controls. By integrating Critical Controls into the planning process, cybersecurity best practice- identified and validated by a broad community of experts- will become the standard.
3. Link roles and controls- The linkage between the enterprise cybersecurity plan and the workforce plan is made by mapping roles (based on a common taxonomy provided by the NICE framework) to the Critical Controls. This yields specific roles necessary to implement various Critical Controls, enabling the development of specific workforce requirements. The heat map analysis also provides additional insight, including which roles can be leveraged to implement a larger number of Controls, or where highly-specialized roles are needed.
4. Define workforce requirements- Enterprise cybersecurity is an enterprise-wide effort. The Essential Tasks Pyramid provides a reference for what each member of the enterprise should be doing, providing a basis of good cyber hygiene. Additionally, the IT operations staff play a crucial role, and their responsibilities- including areas where there is a tension between priorities- must be articulated. Finally, the cybersecurity professionals, including the most technically-sophisticated roles, must be properly selected, trained, developed, placed and supported. Individual capabilities are best reflected by real-world, hands-on experience in a variety of jobs and through performance in competitions. Certifications and education should also be considered as indicators of knowledge and passion.
5. Outline sourcing plan- The workforce can come from within the enterprise or it can be provided by an external party; usually, it is a hybrid. While outsourcing provides many advantages, the overall responsibility for cybersecurity, and thus the performance of the workforce, cannot be outsourced- the enterprise remains primarily accountable for its data and systems. With this in mind, the outsourcing structure and relationship should be managed carefully.
6. Deploy the workforce- The various roles which comprise the workforce must be deployed for maximum positive impact. This includes placement within the organizational structure, assignment of responsibilities and authorities, and

establishment of the reporting chain. The Manpower Map can be referenced to support this process. Effectively deployed, and effectively managed, this workforce will be enabled to deliver maximum value.

7. Maintain governance- Cybersecurity workforce management is not a one-time exercise; rather, it must be an ongoing effort led by senior leaders, including the board of directors and executive management. These leaders can build a security culture, driving and enabling workforce behaviors consistent with good cyber hygiene. By exercising good leadership and implementing workforce management best practices, the enterprise as a whole can improve its cybersecurity posture.

From small start-ups to large multi-national corporations and federal government agencies, all enterprises face common challenges. While each enterprise has its own set of unique circumstances and considerations, the steps outlined in this handbook provide a set of practical guidelines and tips to improve cybersecurity by aligning workforce management to cybersecurity best practice.

A AUTHORS & CONTRIBUTORS

This handbook is the result of a collaborative effort among many writers, reviewers and contributors convened by the Council on CyberSecurity, including subject matter experts on the Roles & Controls panel (http://www.counciloncybersecurity.org/about-us/panels/).

Writers

Geoff Hancock	Advanced Cybersecurity Group
Jim Harris	Obsidian Analysis, Inc.
Maurice Uenuma	Council on CyberSecurity (Co-Chair, Roles & Controls)

Content Contributors

Vilius Benetis	Norway Registers Development CS
Ross Leo	University of Houston- Clear Lake
Billy Rios	Qualys (Co-Chair, Roles & Controls)

Research & Production Team

Adrien Diarra	Georgetown University
Frank Guido	Council on CyberSecurity
Geoff Hancock	Advanced Cybersecurity Group
Anjuri Jha	Council on CyberSecurity
Billy Rios	Qualys (Co-Chair, Roles & Controls)
Charlotte Rodriguez	Council on CyberSecurity
Thomas Sager	Council on CyberSecurity
Maurice Uenuma	Council on CyberSecurity (Co-Chair, Roles & Controls)

Reviewers & Contributors

Maj Linus Barloon, USAF (Ret)	Virginia Tech Applied Research Corporation
Tom Brennan	OWASP, proactiveRISK
Tim Haynes	Children's Hospital Association
Joe Januszewski	WDT
LtCol Sean Kern, USAF	National Defense University
Harold Metzger	Tripwire
Karl Perman	Corporate Risk Solutions, Inc.
Travis Rosiek	FireEye
Rebecca Slayton	Cornell University
Francesca Spidalieri	Pell Center for International Relations and Public Policy
Chris Thompson	Graycon Group
Thomas Vanderhorst, Jr.	Contego Ventures

ABOUT THE COUNCIL ON CYBERSECURITY

The Council on CyberSecurity is an independent, expert, not-for-profit organization with a global scope committed to the security of an open Internet. The Council is committed to the ongoing development and widespread adoption of the Critical Controls, to elevating the competencies of the cybersecurity workforce, and to the development of policies that lead to measurable improvements in our ability to operate safely, securely and reliably in cyberspace. For more information, visit the website at http://www.counciloncybersecurity.org.

B NICE- CRITICAL CONTROLS MAPPING

INTRODUCTION

The National Initiative for Cybersecurity Education (NICE) is a program of the National Institute of Standards and Technology (NIST), designed to address the shortage of qualified cybersecurity professionals in the nation's workforce. Specifically, the National Cybersecurity Workforce Framework (NICE Framework) provides a common taxonomy and reference framework for workforce management across all cybersecurity roles. Defining the cybersecurity profession, through the use of standardized terms and language, facilitates the ability to educate, recruit, train, develop and retain a workforce that is facing critical shortages, in terms of both quantity and capability.

The mapping of cybersecurity roles to Critical Controls was accomplished by aligning knowledge, skills and abilities (KSAs)- the most discrete and foundational units of the NICE framework- to the functions necessary for successful implementation of each Critical Control. This addresses the question of what cybersecurity roles are most involved in implementing the Critical Controls. The mapping serves to align human capital planning to an actionable cybersecurity plan, while further encouraging broad adoption of the NICE framework and reinforcing use of its taxonomy.

NICE FRAMEWORK TAXONOMY

The NICE Framework contains several levels of organization, the smallest and most specific level being the KSAs. These are organized into specialty areas, which also include tasks and competencies. Tasks are unique to each specific specialty area, while competencies and KSAs are not limited to one role; many are repeated across specialty areas. Specialty areas in turn are organized into categories, the highest level of organization in the NICE Framework.

In total, there are 31 specialty areas across seven categories. However, only 24 specialty areas designate tasks and KSAs. The three specialty areas for Collect and Operate (Collection Operations, Cyber Operations and Cyber Operations Planning), and the four for Analyze (Threat Analysis, All Source Intelligence, Exploitation Analysis and Targets), did not include further analysis "due to the unique and highly specialized nature of this work," according to the NICE Framework.

Framework Taxonomy

Label	Definition	Relationship
Cybersecurity Category	A generalized grouping of specialty areas	Can have one or more unique specialty areas associated with a category
Specialty Area (SA)	Defines specific areas of specialty within the cybersecurity domain	•Belongs to one and only one cybersecurity category •Can have any number of unique tasks and KSAs associated with it
Task	Defines high-level activities that codify a specialty area	•Belongs to one and only one cybersecurity specialty area •Tasks are not linked individually to competencies/KSAs
Competency	A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance.	•One or more KSAs are assigned to each competency •The same competency is likely to be needed across multiple specialty areas
KSA	Defines a specific knowledge, skill, ability.	•Assigned to one or more specialty areas •Each KSA has exactly one competency associated with it

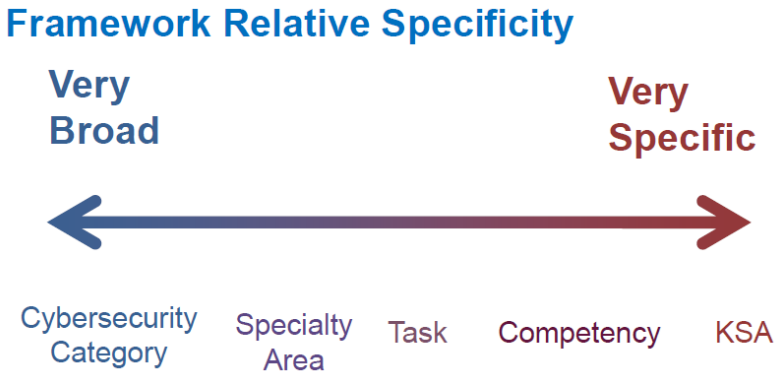


Figure B1 – Framework Taxonomy and Degrees of Specificity[xxiv]

MAPPING METHODOLOGY

The KSAs, being the foundational units of the NICE Framework, were mapped to the Critical Controls. To map the KSAs to the Critical Controls, all 358 unique KSAs were listed regardless of role alignment. Following this listing, using an intentionally inclusive approach, the determination was made if a KSA was applicable or relevant to the implementation and operation of a Critical Control. This process was repeated and subjected to peer review for all 358 KSAs, assessed against each of the 20 Critical Security Controls. The NICE framework categories, Collect & Operate and Analyze, are not included in this mapping due to the aforementioned lack of identified KSAs.

After mapping all the specific KSAs, the specialty areas (as aggregations of KSAs) were linked to the Critical Controls based on KSA alignment. This data was then summarized in a table, from which a heat map was generated to provide a visualization of degrees of alignment and clustering of roles to Critical Controls.

This methodology has several characteristics which influence the resulting data set. Of note, each KSA is weighted equally and degrees of alignment at the specialty area level are a reflection only of the number of KSAs aligned. Therefore, the uniqueness of a KSA (for example, some KSAs appear only in one specific specialty area) is not reflected here. Also, the relative intensity of alignment at the KSA level is not reflected; as mentioned previously, alignment was based on a broadly inclusive determination. As noted in the following section, the validity of this mapping is based primarily on peer and expert review of the findings.

REVIEW AND VALIDATION PROCESS

This methodology was applied by a core team of authors and supporting research analysts (listed in Appendix A), who deliberately mapped roles to Critical Controls at the most discrete level in order to ensure the greatest degree of rigor possible. Where correlation of KSAs to Critical Controls was not obvious, the team was prejudiced toward inclusion.

Throughout the process, the data- both raw data and analysis- was regularly reviewed by the Council's Roles & Controls panel (also listed in Appendix A). This introduced an element of peer review of the analysis, while also infusing the process with Subject Matter Expert (SME) perspective, bringing a valuable practitioner perspective into the work.

THE RAW DATA

Figure B2 below provides a summary display of the number of KSAs in a specialty area that align to each Critical Control, reflecting the aggregate raw data derived through the aforementioned process.

		Critical Security Controls																			
NICE Categories	NICE Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill Gaps	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
Securely Provision	Information Assurance Compliance	10	8	14	11	9	11	9	10	17	10	15	8	16	10	3	1	7	13	12	8
	Software Assurance and Security Engine	13	17	16	10	9	33	10	12	34	11	14	8	22	17	7	6	9	19	24	11
	Systems Security Architecture	26	25	28	18	18	24	29	29	48	34	33	19	37	25	15	16	22	22	39	16
	Technology Research and Development	11	10	15	10	7	20	14	13	27	15	17	11	20	24	12	6	12	17	14	14
	Systems Requirement and Planning	21	22	31	18	17	28	29	26	43	32	31	18	35	28	16	13	17	15	35	18
	Test and Evaluation	9	9	11	8	6	8	8	13	18	11	11	5	12	8	4	5	5	10	17	9
	Systems Development	24	25	28	18	12	24	25	27	49	30	31	19	34	25	15	14	22	19	38	20
Operate and Maintain	Data Administration	7	8	10	6	4	5	4	15	13	6	7	7	6	10	4	2	7	9	17	1
	Knowledge Management	4	4	7	6	6	6	6	8	13	5	6	6	8	5	4	1	3	10	8	4
	Customer Service Tech Support	9	10	13	10	8	6	9	10	12	11	13	7	12	11	6	7	8	12	13	8
	Network Services	20	10	20	9	18	7	32	10	28	34	37	12	37	25	12	6	17	12	29	12
	Systems Administration	15	12	16	9	9	6	15	10	23	18	28	9	21	13	9	5	4	15	19	9
	Systems Security Analysis	16	18	25	18	11	22	22	24	38	24	26	16	32	18	15	11	20	17	33	18
Protect and Defend	CND Analysis	19	17	29	24	31	15	32	20	40	32	38	18	50	32	15	6	13	21	35	19
	Incident Response	4	2	8	8	17	1	9	9	18	9	13	4	19	12	2	3	7	9	17	9
	CND Infrastructure Support	10	8	10	7	17	4	17	7	20	17	20	3	23	11	6	3	8	11	17	7
	Vulnerability Assess & MGMT	8	10	12	16	15	11	10	7	22	10	15	6	22	16	7	1	11	10	20	17
Investigate	Digital Forensics	7	6	12	15	22	15	9	15	35	10	12	10	24	13	6	6	8	19	19	9
	Investigation	1	1	3	3	4	4	2	5	9	2	2	2	5	4	2	1	1	3	8	3
Oversight and Development	Legal Advice and Advocacy	2	2	6	6	6	8	5	5	12	5	4	5	8	2	1	1	1	8	4	4
	Strategic Plan & Policy Dev	4	4	11	9	6	13	7	8	18	7	9	6	12	5	3	1	4	11	8	8
	Education & Training	6	5	7	9	8	8	10	5	18	9	10	5	9	10	7	5	6	12	11	11
	Info Sys Sec Ops (ISSO)	11	13	22	15	13	16	14	16	30	16	21	13	24	21	10	3	11	20	18	10
	Sec Program Mgmt (CISO)	12	13	19	9	13	12	18	19	31	20	24	12	25	22	10	6	11	19	22	12

Figure B2 – NICE Framework to Critical Controls Raw Data Mapping

The far left column lists the NICE Categories, and adjacent to the NICE Categories are columns for the Specialty Areas, color coded according to category. Across the chart as columns are the Critical Controls, starting with Control 1 on the left and ending with Control 20 on the right. Between the specialty area column and the Critical Controls are boxes containing numbers. The number in each box is the number of KSAs from the specialty area on the same horizontal row that align with the Critical Control listed in the vertical column, based on the applicability of that KSA to implementing that specific Control. This raw data was used to produce the heat map for more intuitive visualization of specialty area mapping to Critical Controls.

THE HEAT MAP WITH PERCENTAGES

The heat map below (Figure B3) is a graphic representation of the NICE Specialty Areas that most significantly address the knowledge, skills, and abilities (KSA) associated with each Critical Control. The purpose of this heat map is to present the concentration of KSAs within each Critical Control. The percentages in the cells come from dividing the number of applicable KSAs by the total number of KSAs assigned to that Critical Control; therefore, the percentage for each NICE specialty area represents the percentage of NICE KSAs associated with the specific Critical Control that the specialty area addresses. For example, under Control 1, the KSAs in the Systems Security Architecture specialty area address 30% of all KSAs associated with Control 1.

The "Total" rows for each NICE Category reflect a summation of non-duplicate KSAs at the NICE category level that address each specific Critical Control, enabling further analysis at the aggregate

level. The value in this row is not a sum of all the percentages in each specialty area for that category, rather they are the result of dividing the number of unique KSAs in that category that address the specific Critical Control by the total number of NICE KSAs associated with that Critical Control. Looking at the non-duplicate KSAs for each category shows how a category as a whole can address each Critical Control. This approach provides a higher-level view without specialty area level duplications and enables a more general understanding of where essential roles exist for Critical Controls implementation.

	Critical Security Controls																			
NICE Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill Gaps	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and Services	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
Information Assurance Compliance	9%	9%	11%	10%	8%	9%	8%	9%	7%	8%	9%	10%	8%	6%	4%	2%	9%	9%	6%	9%
Software Assurance and Security Engine	13%	18%	13%	9%	8%	27%	9%	11%	14%	9%	9%	10%	12%	12%	11%	11%	12%	13%	13%	12%
Systems Security Architecture	30%	27%	23%	16%	15%	20%	25%	26%	19%	27%	20%	25%	20%	16%	20%	29%	29%	16%	21%	18%
Technology Research and Development	9%	11%	12%	9%	6%	16%	12%	12%	11%	12%	10%	14%	11%	15%	16%	11%	16%	12%	7%	15%
Systems Requirement and Planning	24%	24%	25%	16%	14%	23%	25%	23%	17%	25%	19%	23%	19%	18%	22%	24%	22%	11%	19%	19%
Test and Evaluation	12%	11%	10%	8%	6%	7%	7%	12%	8%	9%	7%	6%	6%	5%	5%	11%	6%	8%	10%	10%
Systems Development	28%	27%	23%	16%	10%	20%	22%	24%	20%	23%	19%	25%	18%	16%	20%	25%	29%	13%	20%	21%
Total	59%	58%	47%	42%	32%	63%	46%	50%	46%	47%	43%	49%	42%	50%	45%	55%	48%	40%	44%	49%
Data Administration	5%	9%	8%	5%	3%	4%	4%	13%	5%	5%	4%	9%	3%	6%	5%	4%	9%	6%	9%	1%
Knowledge Management	5%	4%	6%	4%	4%	6%	5%	7%	5%	4%	4%	8%	4%	3%	5%	2%	4%	6%	4%	4%
Customer Service Tech Support	10%	11%	10%	9%	7%	5%	8%	9%	5%	9%	8%	9%	6%	7%	8%	13%	10%	9%	7%	9%
Network Services	23%	11%	16%	8%	15%	6%	28%	9%	11%	27%	23%	16%	20%	16%	16%	11%	22%	9%	15%	13%
Systems Administration	6%	5%	4%	3%	3%	2%	4%	3%	4%	5%	6%	4%	4%	4%	5%	4%	2%	5%	4%	3%
Systems Security Analysis	19%	20%	20%	16%	9%	18%	19%	21%	15%	19%	16%	21%	17%	12%	20%	20%	26%	12%	18%	19%
Total	64%	54%	59%	41%	38%	37%	60%	57%	41%	60%	59%	60%	50%	45%	54%	47%	61%	43%	52%	45%
CND Analysis	22%	18%	23%	21%	26%	12%	28%	18%	16%	25%	23%	23%	26%	21%	20%	11%	17%	15%	19%	20%
Incident Response	5%	2%	6%	7%	14%	1%	8%	8%	7%	7%	8%	5%	10%	8%	3%	5%	9%	6%	9%	10%
CND Infrastructure Support	12%	9%	8%	6%	14%	3%	15%	6%	8%	13%	12%	4%	12%	7%	8%	5%	10%	8%	9%	7%
Vulnerability Assess & MGMT	9%	11%	10%	14%	13%	9%	9%	6%	9%	8%	9%	8%	12%	10%	9%	2%	14%	7%	11%	18%
Total	31%	27%	31%	32%	39%	20%	39%	23%	24%	34%	33%	30%	38%	29%	28%	16%	29%	21%	29%	30%
Digital Forensics	8%	7%	10%	13%	18%	12%	8%	13%	15%	8%	7%	13%	13%	8%	8%	11%	10%	13%	10%	10%
Investigation	1%	1%	2%	3%	3%	3%	2%	4%	4%	2%	1%	3%	3%	3%	3%	2%	1%	2%	4%	3%
Total	9%	8%	11%	15%	19%	14%	9%	14%	15%	9%	8%	14%	14%	10%	9%	13%	12%	16%	12%	12%
Legal Advice and Advocacy	2%	2%	5%	5%	5%	7%	4%	4%	5%	4%	2%	6%	4%	1%	1%	2%	1%	6%	2%	4%
Strategic Plan & Policy Dev	5%	4%	9%	8%	5%	11%	6%	7%	7%	5%	6%	8%	6%	3%	4%	2%	5%	8%	4%	9%
Education & Training	7%	5%	6%	8%	7%	7%	9%	4%	7%	7%	6%	6%	5%	6%	9%	9%	8%	9%	6%	12%
Info Sys Sec Ops (ISSO)	13%	14%	18%	13%	11%	13%	12%	14%	12%	13%	13%	17%	13%	14%	14%	5%	14%	14%	10%	11%
Sec Program Mgmt (CISO)	14%	14%	15%	8%	11%	10%	16%	17%	13%	16%	15%	16%	13%	14%	14%	11%	14%	13%	12%	13%
Total	27%	25%	32%	28%	26%	26%	28%	28%	30%	27%	27%	30%	26%	26%	30%	25%	31%	33%	23%	32%
Total # of KSA for each Control	86	92	124	114	119	123	114	113	247	128	162	77	189	155	74	55	77	141	188	94

*The number of total KSAs refers to the number of unique KSAs that were assigned to each Control

Figure B3- Heat Map of NICE Specialty Areas to Critical Security Controls

Summary of overall methodology for this mapping:

1. Mapping of KSAs for each specialty area to each Critical Control
2. Summation of all KSAs associated with each Critical Control
3. Heat mapping by NICE specialty areas and by NICE categories (as addressed above)
4. Analysis

OBSERVATIONS AND ANALYSIS

As the category totals show, the majority of Controls can be significantly addressed by implementing the NICE specialty areas in the Securely Provision and Operate & Maintain categories. An obvious exception to this is Critical Control 5 (Malware Defenses), which appears to be most addressed by the specialty areas in the Protect & Defend category.

- Not surprisingly, Critical Control 6 (Software Application Security) shows a high degree of alignment with Software Security and Engineering. This high correlation appears to be an outlier for both the Critical Control and specialty area.
- Surprisingly, there is only an average degree of alignment of Education and Training and Security Program Management (CISO) to Critical Control 9 (Security Skills Assessment), which is focused primarily on cybersecurity personnel.
- For Critical Control 18 (Incident Response and Management) there is a remarkably low degree of alignment with the Incident Response specialty area (Protect & Defend). In fact, Critical Control 18 doesn't appear highly aligned anywhere, including the specialty areas Digital Forensics and Investigation, which would seem to only align to Critical Control 18.
- There is a relatively low alignment of Test and Evaluation to Critical Control 20 (Penetration Testing). This is a reflection of the low number of KSAs associated with System Administration despite their importance. Results like this suggest the need for further analysis at the KSA level to identify or to properly weight the significance of each KSA.
- Total rows for each NICE category can be used as an initial indication of KSA overlap among specialty areas in that Category. For example, the first column (Critical Control 1) for the first category (Securely Provision) contains values that sum to 125% but the total for the Securely Provision category is only 52%. As the Total value for each category only accounts for non-duplicate KSAs in that category that address Critical Control 1, this difference indicates that there is a large amount of KSA overlap (or duplication) among the specialty areas in that category.
- The five specialty areas that on average address the most Critical Control KSAs, in order of significance, are:
    - 22% - Systems Security Architecture (Securely Provision)
    - 21% - Systems Requirement and Planning (Securely Provision)
    - 21% - Systems Development (Securely Provision)
    - 20% - CND Analysis (Protect and Defend)
    - 18% - Systems Security Analysis (Operate and Maintain)
- The specialty areas in Securely Provision have a greater tendency to address the KSAs for Critical Controls, with the largest amount of KSA overlap of any category. The high degree of alignment across the entire row for some specialty areas suggests a high concentration of generic, redundant KSAs. This could indicate the broad coverage of essential Critical Controls-related KSAs by a relatively small number of roles, subject to further analysis at the KSA level. This overlap may be cause to consider collapsing or consolidating a few of these roles. For enterprise workforce planning, this suggests the opportunity to leverage a smaller number of roles to apply the KSAs necessary to implement a set of Critical Controls.

- The specialty areas in the Operate and Maintain category have less overlap, but as a whole, this category addresses the largest percentage of KSAs, accounting for 60% of the total. This suggests that each specialty area is necessary to holistically address the KSAs necessary to implement the Critical Controls. An example of the degree of KSA uniqueness for the Operate & Maintain category is the fact that while there are fewer specialty areas associated with this category (six versus seven for Securely Provision) the alignment of KSAs at the category level is still higher than Securely Provision in most cases.

ALTERNATIVE HEAT MAP SHOWING DISTRIBUTION BY SPECIALTY AREA

Figure B4 is the Distribution by Specialty Area Heat Map. The color scale is white to red with the color white indicating a low percentage and the dark red indicating a higher percentage. This heat map shows the percentage of KSAs contained in a specialty area (horizontally across the table) aligning with each Critical Control. For example, the specialty area Information Assurance Compliance contains a total of 19 KSAs. By referencing Figure B4, one sees that there are 10 KSAs from specialty area Information Assurance Compliance that align with Critical Control 1. Ten KSAs out of a total of 19 KSAs align with Critical Control 1, thereby providing the 53%. Each specialty area has its own color scale, horizontally aligned within the row.

Advantages: By accounting for the total number of KSA's in each specialty area, this heat map shows the relative degree of alignment of specialty areas to each Critical Control.

Disadvantages: This heat map skews in favor of specialty areas with lower numbers of KSAs. For example, a specialty area that has 3 KSA's aligned out of a total of 5 KSAs will have a higher percentage and darker color than a specialty area that has 6 KSAs aligned out of a total of 12 KSAs. Another disadvantage of this heat map is that the descriptions of the KSAs range across a spectrum of specific to vague. This heat map skews heavily towards the specialty areas that could be considered to contain the most vaguely described KSAs. These vaguely described KSAs show extremely high alignment across most or all of the Critical Controls.

For these reasons, this version of the heat map was not used in the final analysis.

		Critical Security Controls																			
NICE Categories	NICE Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill Gaps	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
Securely Provision	Information Assurance Compliance	53%	42%	74%	58%	47%	58%	47%	53%	89%	53%	79%	42%	84%	53%	16%	5%	37%	68%	63%	42%
	Software Assurance and Security Engine	28%	36%	34%	21%	19%	70%	21%	26%	72%	23%	30%	17%	47%	36%	15%	13%	19%	40%	51%	23%
	Systems Security Architecture	52%	50%	56%	36%	36%	48%	58%	58%	96%	68%	66%	38%	74%	50%	30%	32%	44%	44%	78%	32%
	Technology Research and Development	30%	27%	41%	27%	19%	54%	38%	35%	73%	41%	46%	30%	54%	65%	32%	16%	32%	46%	38%	38%
	Systems Requirement and Planning	43%	45%	63%	37%	35%	57%	59%	53%	88%	65%	63%	37%	71%	57%	33%	27%	35%	31%	71%	37%
	Test and Evaluation	43%	43%	52%	38%	29%	38%	38%	62%	86%	52%	52%	24%	57%	38%	19%	24%	24%	48%	81%	43%
	Systems Development	44%	45%	51%	33%	22%	44%	45%	49%	89%	55%	56%	35%	62%	45%	27%	25%	40%	35%	69%	36%
Operate and Maintain	Data Administration	30%	35%	43%	26%	17%	22%	17%	65%	57%	26%	30%	30%	26%	43%	17%	9%	30%	39%	74%	4%
	Knowledge Management	27%	27%	47%	40%	40%	40%	40%	53%	87%	33%	40%	40%	53%	33%	27%	7%	20%	67%	53%	27%
	Customer Service Tech Support	56%	63%	81%	63%	50%	38%	56%	63%	75%	69%	81%	44%	75%	69%	38%	44%	50%	75%	81%	50%
	Network Services	53%	26%	53%	24%	47%	18%	84%	26%	74%	89%	97%	32%	97%	66%	32%	16%	45%	32%	76%	32%
	Systems Administration	42%	33%	44%	25%	25%	17%	42%	28%	64%	50%	78%	25%	58%	36%	25%	14%	11%	42%	53%	25%
	Systems Security Analysis	36%	41%	57%	41%	25%	50%	50%	55%	86%	55%	59%	36%	73%	41%	34%	25%	45%	39%	75%	41%
Protect and Defend	CND Analysis	31%	28%	48%	39%	51%	25%	52%	33%	66%	52%	62%	30%	82%	52%	25%	10%	21%	34%	57%	31%
	Incident Response	17%	8%	33%	33%	71%	4%	38%	38%	75%	38%	54%	17%	79%	50%	8%	13%	29%	38%	71%	38%
	CND Infrastructure Support	38%	31%	38%	27%	65%	15%	65%	27%	77%	65%	77%	12%	88%	42%	23%	12%	31%	42%	65%	27%
	Vulnerability Assess & MGMT	25%	31%	38%	50%	47%	34%	31%	22%	69%	31%	47%	19%	69%	50%	22%	3%	34%	31%	63%	53%
Investigate	Digital Forensics	13%	11%	22%	27%	40%	27%	16%	27%	64%	18%	22%	18%	44%	24%	11%	11%	15%	35%	35%	16%
	Investigation	8%	8%	25%	25%	33%	33%	17%	42%	75%	17%	17%	17%	42%	33%	17%	8%	8%	25%	67%	25%
Oversight and Development	Legal Advice and Advocacy	15%	15%	46%	46%	46%	62%	38%	38%	92%	38%	31%	38%	62%	15%	8%	8%	8%	62%	31%	31%
	Strategic Plan & Policy Dev	22%	22%	61%	50%	33%	72%	39%	44%	100%	39%	50%	33%	67%	28%	17%	6%	22%	61%	44%	44%
	Education & Training	33%	28%	39%	50%	44%	44%	56%	28%	100%	50%	56%	28%	50%	56%	39%	28%	33%	67%	61%	61%
	Info Sys Sec Ops (ISSO)	35%	42%	71%	48%	42%	52%	45%	52%	97%	52%	68%	42%	77%	68%	32%	10%	35%	65%	58%	32%
	Sec Program Mgmt (CISO)	36%	39%	58%	27%	39%	36%	55%	58%	94%	61%	73%	36%	76%	67%	30%	18%	33%	58%	67%	36%

Figure B4 – Heat Map by Distribution within Each Specialty Area

SPECIALTY AREAS WITH NO KSAS

Of the 31 Specialty Areas contained in the NICE framework, seven do not have any KSAs associated with them. The seven Specialty Areas with no KSAs are: Collection Operations, Cyber Operations Planning, Cyber Operations, Threat Analysis, Exploitation Analysis, All Source Intelligence, and Targets. The NICE framework explains that due to the unique and highly specialized nature of the work associated with these seven categories, task and KSA-level content is not provided.

To provide a linkage between these seven specialty areas and the Critical Controls, a survey was conducted of the SMEs comprising the Roles & Controls panel. The survey asked panelists to indicate the degree that the seven specialty areas aligned with the Critical Controls. The responses to the survey were compiled to produce the heat map below (Figure B5):

		Critical Security Controls																		
NICE Category	Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill Gaps	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and Services	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
Collect & Operate	Collection Operations	4.67	4.33	4.33	4.67	3.33	3.00	3.67	3.00	3.67	3.50	3.67	2.33	4.00	4.33	2.67	4.00	4.00	4.33	2.67	3.00
	Cyber Operations Planning	3.00	2.67	3.00	4.00	3.33	3.00	3.67	3.67	3.67	2.67	2.67	3.00	4.00	3.67	2.33	2.67	2.33	3.00	1.67	3.00
	Cyber Operations	3.33	3.33	3.67	4.67	4.00	2.33	3.67	3.00	2.33	3.33	2.33	3.00	4.67	3.33	2.33	3.33	3.00	3.67	2.33	2.33
Analyze	Threat Analysis	4.00	4.00	4.33	3.67	4.67	4.67	3.67	3.00	3.33	3.33	3.67	2.67	5.00	4.00	2.33	4.00	4.00	3.67	5.00	5.00
	Exploitation Analysis	4.00	2.67	3.00	4.33	4.00	3.67	4.33	3.33	2.67	3.67	3.33	2.00	3.67	3.00	1.67	3.00	2.67	4.33	3.33	4.00
	All Source Intelligence	2.67	3.00	2.67	2.67	4.67	3.33	3.33	3.33	2.00	3.33	3.00	3.00	4.00	3.67	2.00	2.33	2.67	3.00	2.67	4.00
	Targets	2.33	2.67	3.00	3.33	4.33	2.33	2.67	2.33	2.33	2.67	1.33	1.00	3.33	2.67	2.00	1.67	2.00	4.00	2.67	3.67

Figure B5 – Heat Map by Distribution for Specialty Areas with no KSAs

FINAL HEAT MAP

The heat map below (Figure B6) shows the degree of concentration of aligned KSAs from each specialty area to each Critical Control, supported and supplemented by the input of SMEs on the Council's Roles & Controls panel. This is a combination of the heat maps presented in Figure B3 and Figure B5. It is also simplified by removing raw data or percentages and replacing them with single digits to reflect degrees of alignment.

Degrees of Alignment

Lower 1 2 3 4 5 Higher

NICE Categories	NICE Specialty Areas	1-Inventory of Authorized and Unauthorized Devices	2-Inventory of Authrized and Unauthorized Software	3-Secure Configurations for Hardware and Software	4-Continuous Vulnerability Assessment and Remediation	5-Malware Defenses	6-Application Software Security	7-Wireless Access Control	8-Data Recovery Capability	9-Security Skills Assessment and Appropriate Training to Fill	10-Secure Configurations for Network Devices	11-Limitation and Control of Network Ports, Protocols, and	12-Controlled Use of Administrative Privileges	13-Boundary Defense	14-Maintenance, Monitoring, and Analysis of Audit Logs	15-Controlled Access Based on the Need to Know	16-Account Monitoring and Control	17-Data Protection	18-Incident Response and Management	19-Secure Network Engineering	20-Penetration Tests and Red Team Exercises
		Critical Security Controls																			
Securely Provision	Information Assurance Compliance	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	2	2	2
	Software Assurance and Security Engineering	3	4	3	2	2	5	2	2	3	2	2	2	2	2	2	2	2	3	3	2
	Systems Security Architecture	5	5	4	3	3	4	5	5	4	5	4	5	4	3	4	5	5	3	4	4
	Technology Research and Development	2	2	3	2	1	3	3	2	2	2	2	3	2	3	3	2	3	3	2	3
	Systems Requirement and Planning	5	4	5	3	3	4	5	4	3	5	4	4	4	4	4	4	4	2	4	4
	Test and Evaluation	2	2	2	2	1	2	2	3	2	2	2	2	2	1	1	2	2	2	2	2
	Systems Development	5	5	4	3	2	4	4	4	4	4	4	5	3	3	4	5	5	3	2	4
Operate and Maintain	Data Administration	1	2	2	1	1	1	1	3	1	1	1	2	1	2	1	1	2	2	2	1
	Knowledge Management	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	2	1	1
	Customer Service Tech Support	2	2	2	2	2	1	2	2	1	2	2	2	2	2	2	3	2	2	2	2
	Network Services	4	2	3	2	3	1	5	2	2	5	4	3	4	3	3	2	4	2	3	3
	Systems Administration	3	3	3	2	2	1	3	2	2	3	3	2	2	2	3	2	1	2	2	2
	Systems Security Analysis	4	4	4	3	2	3	4	4	3	4	3	4	3	2	4	4	5	3	3	4
Protect and Defend	CND Analysis	4	4	4	4	5	3	5	3	3	5	4	4	5	4	4	2	3	3	4	4
	Incident Response	1	1	2	2	3	1	2	2	2	2	2	1	2	2	1	1	2	2	2	2
	CND Infrastructure Support	2	2	2	2	3	1	3	2	2	3	3	1	3	2	2	1	2	2	2	2
	Vulnerability Assess & Management	2	2	2	3	3	2	2	2	2	2	2	2	2	2	2	1	3	2	2	4
Investigate	Digital Forensics	2	2	2	3	4	3	2	3	3	2	2	3	3	2	2	2	2	3	2	2
	Investigation	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Collect & Operate	Collection Operations	5	4	4	5	3	3	4	3	4	4	4	2	4	4	3	4	4	4	3	3
	Cyber Operations Planning	3	3	3	4	3	3	4	4	4	3	3	3	4	4	2	3	2	3	2	3
	Cyber Operations	3	3	4	5	4	2	4	3	2	3	2	3	5	3	2	3	3	4	2	2
Analyze	Threat Analysis	4	4	4	4	5	5	4	3	3	3	4	3	5	4	2	4	4	4	5	5
	Exploitation Analysis	4	3	3	4	4	4	4	3	3	4	3	2	4	3	2	3	3	4	3	4
	All Source Intelligence	3	3	3	3	5	3	3	3	2	3	3	3	4	4	2	2	3	3	3	4
	Targets	2	3	3	3	4	2	3	2	2	3	1	1	3	3	2	2	2	4	3	4
Oversight and Development	Legal Advice and Advocacy	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1
	Strategic Plan & Policy Dev	1	1	2	2	1	2	2	2	2	1	1	2	2	1	1	1	1	2	1	2
	Education & Training	2	1	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	1	2
	Info Sys Sec Ops (ISSO)	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	1	3	3	2	2
	Sec Program Mgmt (CISO)	3	3	3	2	2	2	3	3	3	3	3	3	3	3	3	2	3	3	2	3

Figure B6 – Final Heat Map

C ROLES FOR EACH CRITICAL CONTROL

The following is a by-Control analysis of workforce needs, based on the mapping of NICE Specialty Areas to Critical Controls presented in Appendix B. This section provides individual "tear sheets" for understanding which roles are necessary for implementing each Control, linking enterprise workforce planning alignment with enterprise cybersecurity planning. As specific Controls are prioritized based on risk profile and security strategy, this section provides a summary of the roles and skillsets necessary.

Critical Security Control 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 30%- Information Assurance (IA) Architect, Information Systems Security Engineer, Systems Security Analyst

2. Systems Development (Securely Provision), 28%- Firewall Engineer, Information Assurance (IA) Software Engineer, Information Systems Security Engineer

3. Systems Requirement and Planning (Securely Provision), 24% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. Network Services (Operate and Maintain), 23%- Network Systems Engineer, Systems Engineer, Network Administrator

5. CND Analysis (Protect and Defend), 22%- Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

Critical Security Control 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 27% - Information Assurance (IA) Architect, Information Security Architect, Research & Development Engineer

2. Systems Development (Securely Provision), 27% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

3. Systems Requirement and Planning (Securely Provision), 24% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. Systems Security Analysis (Operate and Maintain), 20% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

5. Software Assurance and Security Engineering (Securely Provision), 18% - Computer Programmer, Information Assurance (IA) Software Developer, Software Engineer/Architect

Critical Security Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Requirements and Planning (Securely Provision), 25% – Business Process Analyst, Computer Systems Analyst, Requirements Analyst, Human Factors Engineer

2. Systems Security Architecture (Securely Provision), 23% - Information Assurance (IA) Architect, Information Security Architect, Research & Development Engineer

3. Systems Development (Securely Provision), 23% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

4. CND Analysis (Protect and Defend), 23% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

5. Systems Security Analysis (Operate and Maintain), 20% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. CND Analysis (Protect and Defend), 21% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

2. Systems Security Architecture (Securely Provision), 16% - Information Assurance (IA) Architect, Information Security Architect, Research & Development Engineer

3. Systems Requirements and Planning (Securely Provision), 16% – Business Process Analyst, Computer Systems Analyst, Requirements Analyst, Human Factors Engineer

4. Systems Development (Securely Provision), 16% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

5. Systems Security Analysis (Operate and Maintain), 16% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 5: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. CND Analysis (Protect and Defend), 26% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

2. Digital Forensics (Investigate), 18% – Computer Forensic Analyst, Digital Forensic Examiner, Network Forensic Examiner

3. Systems Security Architecture (Securely Provision), 15% - Information Assurance (IA) Architect, Information Security Architect, Information Systems Security Engineer

4. Network Services (Operate and Maintain), 15% - Cabling Technician, Network Designer, Network Engineer

5. Systems Requirement and Planning (Securely Provision), 14% - Requirements Analyst, Systems Consultant, Systems Engineer

Critical Security Control 6: Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Software Assurance and Security Engineering (Securely Provision), 27% - Computer Programmer, Information Assurance (IA) Software Developer, Software Engineer/Architect

2. Systems Requirement and Planning (Securely Provision), 23% - Computer Systems Analyst, Solutions Architect, Systems Engineer

3. Systems Security Architecture (Securely Provision), 20% - Information Assurance (IA) Architect, Information Security Architect, Research & Development Engineer

4. Systems Development (Securely Provision), 20% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

5. Systems Security Analysis (Operate and Maintain), 18% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 7: Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Network Services (Operate and Maintain), 28% - Cabling Technician, Network Designer, Network Engineer

2. CND Analysis (Protect and Defend), 28% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

3. Systems Security Architecture (Securely Provision), 25% - Information Assurance (IA) Architect, Systems Engineer, Systems Security Analyst

4. Systems Requirement and Planning (Securely Provision), 25% - Human Factors Engineer, Requirements Analyst, Solutions Architect

5. Systems Development (Securely Provision), 22% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

Critical Security Control 8: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 26% - Information Systems Security Engineer, Security Solutions Architect, Systems Security Analyst

2. Systems Development (Securely Provision), 24% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

3. Systems Requirement and Planning (Securely Provision), 23% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

4. Systems Security Analysis (Operate and Maintain), 21% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

5. CND Analysis (Protect and Defend), 18% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

Critical Security Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Development (Securely Provision), 20% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

2. Systems Security Architecture (Securely Provision), 19% - Information Assurance (IA) Architect, Information Systems Security Engineer, Systems Security Analyst

3. Systems Requirement and Planning (Securely Provision), 17% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. CND Analysis (Protect and Defend), 16% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

5. Systems Security Analysis (Operate and Maintain), 15% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 27% - Information Assurance (IA) Architect, Information Security Architect, Information Systems Security Engineer

2. Network Services (Operate and Maintain), 27% - Cabling Technician, Network Designer, Network Engineer

3. Systems Requirement and Planning (Securely Provision), 25% - Requirements Analyst, Systems Consultant, Systems Engineer

4. CND Analysis (Protect and Defend), 25% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

5. Systems Development (Securely Provision), 23% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

Critical Security Control 11: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Network Services (Operate and Maintain), 23% - Cabling Technician, Converged Network Engineer, Network Administrator

2. CND Analysis (Protect and Defend), 23% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

3. Systems Security Architecture (Securely Provision), 20% - Security Solutions Architect, Information Assurance (IA) Architect, Information Systems Security Engineer

4. Systems Requirement and Planning (Securely Provision), 19% - Business Process Analyst, Computer Systems Analyst, Solutions Architect

5. Systems Development (Securely Provision), 19% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

Critical Security Control 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Highest aligned NICE Framework Specialty Areas and associated Job Titles

1. Systems Security Architecture (Securely Provision), 25% - Information Assurance (IA) Architect, Information Systems Security Engineer, Systems Security Analyst

2. Systems Development (Securely Provision), 25% - Firewall Engineer, Information Assurance (IA) Software Engineer, Information Systems Security Engineer

3. Systems Requirement and Planning (Securely Provision), 23% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. CND Analysis (Protect and Defend), 23% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

5. Systems Security Analysis (Operate and Maintain), 21% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 13: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. CND Analysis (Protect and Defend), 26% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

2. Systems Security Architecture (Securely Provision), 20% - Information Assurance (IA) Architect, Systems Engineer, Systems Security Analyst

3. Network Services (Operate and Maintain), 20% - Cabling Technician, Converged Network Engineer, Network Administrator

4. Systems Requirement and Planning (Securely Provision), 19% - Human Factors Engineer, Requirements Analyst, Solutions Architect

5. Systems Development (Securely Provision), 18% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

Critical Security Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. CND Analysis (Protect and Defend), 21% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

2. Systems Requirement and Planning (Securely Provision), 18% - Business Process Analyst, Computer Systems Analyst, Solutions Architect

3. Systems Security Architecture (Securely Provision), 16% - Information Assurance (IA) Architect, Systems Engineer, Systems Security Analyst

4. Systems Development (Securely Provision), 16% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

5. Network Services (Operate and Maintain), 16% - Network Systems Engineer, Systems Engineer, Network Administrator

Critical Security Control 15: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Requirement and Planning (Securely Provision), 22% - Business Process Analyst, Computer Systems Analyst, Solutions Architect

2. Systems Security Architecture (Securely Provision), 20% - Information Assurance (IA) Architect, Systems Engineer, Systems Security Analyst

3. Systems Development (Securely Provision), 20% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

4. Systems Security Analysis (Operate and Maintain), 20% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

5. CND Analysis (Protect and Defend), 20% -Cybersecurity Intelligence Analyst, Incident Analyst, Network Defense Technician

Critical Security Control 16: Account Monitoring and Control

Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 29% - Information Assurance (IA) Architect, Systems Engineer, Systems Security Analyst

2. Systems Development (Securely Provision), 25% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

3. Systems Requirement and Planning (Securely Provision), 24% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. Systems Security Analysis (Operate and Maintain), 20% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

5. Customer Service and Technical Support (Operate and Maintain), 13% - Computer Support Specialist, Systems Administrator, User Support Specialist

Critical Security Control 17: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 29% - Security Solutions Architect, Information Assurance (IA) Architect, Information Systems Security Engineer

2. Systems Development (Securely Provision), 29% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

3. Systems Security Analysis (Operate and Maintain), 26% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

4. Systems Requirement and Planning (Securely Provision), 22% - Business Process Analyst, Computer Systems Analyst, Solutions Architect

5. Network Services (Operate and Maintain), 22% - Cabling Technician, Network Designer, Network Engineer

Critical Security Control 18: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 16% - Information Systems Security Engineer, Network Security Analyst, Systems Engineer

2. CND Analysis (Protect and Defend), 15% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

3. Information Security Systems Operations (Oversight and Development), 14% – Information Assurance (IA) Manager, Information Assurance (IA) Security Officer, Information Systems Security Officer (ISSO)

4. Software Assurance and Security Engineering (Securely Provision), 13% - Computer Programmer, Information Assurance (IA) Software Developer, Software Engineer/Architect

5. Systems Development (Securely Provision), 13% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

Critical Security Control 19: Secure Network Engineering

Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Security Architecture (Securely Provision), 21% - Information Assurance (IA) Architect, Information Security Architect, Information Systems Security Engineer

2. Systems Development (Securely Provision), 20% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

3. Systems Requirement and Planning (Securely Provision), 19% - Business Process Analyst, Computer Systems Analyst, Systems Consultant

4. CND Analysis (Protect and Defend), 19% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

5. Systems Security Analysis (Operate and Maintain), 18% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

Critical Security Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Highest aligned NICE Framework Specialty Areas with associated Job Titles

1. Systems Development (Securely Provision), 21% - Information Assurance (IA) Developer, Information Assurance (IA) Engineer, Information Assurance (IA) Software Engineer

2. CND Analysis (Protect and Defend), 20% - Computer Network Defense (CND) Analyst (Cryptologic), Incident Analyst, Network Defense Technician

3. Systems Requirement and Planning (Securely Provision), 19%- Business Process Analyst, Computer Systems Analyst, Solutions Architect

4. Systems Security Analysis (Operate and Maintain), 19% - Information Systems Security Manager (ISSM), Information Assurance (IA) Operational Engineer, Information Security Specialist

5. Systems Security Architecture (Securely Provision), 18% - Information Assurance (IA) Architect, Information Security Architect, Research & Development Engineer

5. Vulnerability Assessment and Management (Protect and Defend), 18% - Computer Network Defense (CND) Auditor, Risk/Vulnerability Analyst, Technical Surveillance Countermeasures Technician

D REFERENCES

Aguilar, Luis A. 2014. "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus." *"Cyber Risks and the Boardroom" Conference.* New York, New York, June 10. http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_edn12.

Ashraf, Salman. 2005. *Organization Need and Everyone's Responsibility Information Security Awareness.* SANS Whitepaper, SANS Institute. http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113.

Beechey, Jim. 2014. "Using the Critical Security Controls to Measure and Fund Your Program." *www.councilоncybersecurity.org.* September 2. Accessed September 17, 2014. http://www.councilоncybersecurity.org/articles/using-the-critical-security-controls-to-measure-and-fund-your-program/.

Cisco. 2014. *Cisco 2014 Annual Security Report.* Report, Cisco .

Council on CyberSecurity. 2014. *Critical Security Controls for Effective Cyber Defense Version 5.0.* Cybersecurity Report, Council on CyberSecurity. http://www.councilоncybersecurity.org/critical-controls/.

Garrett, Chris. 2004. *Developing a Security Awareness Culture- Improving Security Decision Making.* SANS Whitepaper, SANS Institute. http://www.sans.org/reading-room/whitepapers/awareness/developing-security-awareness-culture-improving-security-decision-making-1526.

Harvard Business Review. 2013. *Meeting the Cyber Risk Challenge.* Harvard Business Review Analytic Services Report, Harvard Business School Publishing.

Hoemeyer, Jane; Maxson, Margaret;. 2011. "Introduction to NICE Cybersecurity Workforce Framework." *http://csrc.nist.gov/.* September 20. Accessed October 6, 2014. http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Wednesday/Wed_Intro-Framework_Maxson_Homeyer_Mills.pdf.

Homeland Security Advisory Council. 2012. *Cyber Skills Task Force Report.* Taskforce Report, Department of Homeland Security.

Kern, Sean, and Francesca Spidalieri. 2014. *Professionalizing Cybersecurity: A path to universal standards and status.* Report, Newport, RI: Salve Regina University, Pell Center for International Relations and Public Policy.

Lloyd's. 2013. *Lloyd's Risk Index 2013.* Ipsos SA. Accessed September 11, 2014. http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf.

Lute, Jane, Deirdre Durrance, and Maurice Uenuma. 2014. *Mission Critical CyberSecurity Functions.* Paper, Council on CyberSecurity.

Mandiant: A FireEye Company. 2014. *M Trends: Beyond the Breach.* Mandiant: A FireEye Company.

National Association of Corporate Directors. 2014. *Cybersecurity: Boardroom Implications.* Report, Washington, D.C.: National Association of Corporate Directors.

National Institute of Standards and Technology. 2010. *Guide to Applying the Risk Management Framework to Federal Information Systems.* NIST Special Publication, NIST U.S. Chamer of Commerce. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

O'Connor, Clare. 2014. "Target CEO Gregg Steinhafel Resigns In Data Breach Fallout." *www.forbes.com.* May 5. Accessed September 11, 2014. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/.

Ponemon Institute. 2012. *2012 Cost of Cyber Crime Study: United States.* Research Report, Ponemon Institute.

Ponemon Institute LLC. 2014. *Cybersecurity Incident Response: Are we as prepared as we think?* Research Report, Ponemon Institute. Accessed September 11, 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.

PricewaterhouseCoopers LLP. 2014. *Defending yesterday Key findings from the Global State of Information Security Survey 2014.* Survey Report, PricewaterhouseCoopers.

Project Management Institute. 2006. *Practice Standard for Workforce Breakdown Structures-2nd Edition.* Publication, Newton Square, PA: Project Management Institute, Inc.

Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. 2014. *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It.* March 13. Accessed September 23, 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Rosch, Fran. 2014. "Prepared Testimony and Statement for the Record, Hearing on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cyber Crime" before the U.S. Senate Committee on the Judiciary." Symantec Corporation, February.

Suby, Michael. 2013. *The 2013 (ISC)² Global Information Security Workforce Study.* Market Study, A Frost and Sullivan Market Study in Partnership with (ISC)² and Booz Allen Hamilton.

Tarala, James. September, 2014. *Critical Security Controls: From Adoption to Implementation.* SANS Institute Analyst Survey, SANS Institute.

Verizon Communications . 2014. *2014 Data Breach Investigations Report.* Report, Verizon Communications.

Verizon Communications. 2012. *2012 Data Breach Investigations Report.* Report, Verizon Communications.

Worland, Justin. 2014. *How That Massive Celebrity Hack Might Have Happened.* September 1. Accessed September 17, 2014. http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/.

E NOTES

[i] Ponemon Institute. 2012. 2012 Cost of Cyber Crime Study: United States. Research Report, Ponemon Institute.

[ii] National Institute of Standards and Technology. 2010. Guide to Applying the Risk Management Framework to Federal Information Systems. NIST Special Publication, NIST U.S. Chamber of Commerce. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[iii]Lloyd's. 2013. Lloyd's Risk Index 2013. Ipsos SA. Accessed September 11, 2014. http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf.

[iv] Ponemon Institute LLC. 2014. Cybersecurity Incident Response: Are we as prepared as we think? Research Report, Ponemon Institute. Accessed September 11, 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.

[v] Tarala, James. September, 2014. Critical Security Controls: From Adoption to Implementation. SANS Institute Analyst Survey, SANS Institute.

[vi] Ibid

[vii] Aguilar, Luis A. 2014. "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus." "Cyber Risks and the Boardroom" Conference. New York, New York, June 10. http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_edn12.

[viii]O'Connor, Clare. 2014. "Target CEO Gregg Steinhafel Resigns In Data Breach Fallout." www.forbes.com. May 5. Accessed September 11, 2014. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/.

[ix] Harvard Business Review. 2013. Meeting the Cyber Risk Challenge. Harvard Business Review Analytic Services Report, Harvard Business School Publishing.

[x] Verizon Communications. 2014. *2014 Data Breach Investigations Report.* Report, Verizon Communications.

[xi] Mandiant: A FireEye Company. 2014. M Trends: Beyond the Breach. Mandiant: A FireEye Company.

[xii] Council on CyberSecurity. 2014. Critical Security Controls for Effective Cyber Defense Version 5.0. Cybersecurity Report, Council on CyberSecurity. http://www.counciloncybersecurity.org/critical-controls/.

[xiii] Project Management Institute. 2006. Practice Standard for Workforce Breakdown Structures-2nd Edition. Publication, Newton Square, PA: Project Management Institute, Inc.

[xiv] Suby, Michael. 2013. The 2013 $(ISC)^2$ Global Information Security Workforce Study. Market Study, A Frost and Sullivan Market Study in Partnership with $(ISC)^2$ and Booz Allen Hamilton.

[xv] Homeland Security Advisory Council. 2012. Cyber Skills Task Force Report. Taskforce Report, Department of Homeland Security.

[xvi] Lute, Jane, Deirdre Durrance, and Maurice Uenuma. 2014. Mission Critical CyberSecurity Functions. Paper, Council on CyberSecurity.

[xvii] Kern, Sean, and Francesca Spidalieri. 2014. *Professionalizing Cybersecurity: A path to universal standards and status.* Report, Newport, RI: Salve Regina University, Pell Center for International Relations and Public Policy.

[xviii] Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. 2014. Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. March 13. Accessed September 23, 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[xix] National Association of Corporate Directors. 2014. Cybersecurity: Boardroom Implications. Report, Washington, D.C.: National Association of Corporate Directors.

[xx] Garrett, Chris. 2004. Developing a Security Awareness Culture- Improving Security Decision Making. SANS Whitepaper, SANS Institute. http://www.sans.org/reading-room/whitepapers/awareness/developing-security-awareness-culture-improving-security-decision-making-1526.

[xxi] Ashraf, Salman. 2005. Organization Need and Everyone's Responsibility Information Security Awareness. SANS Whitepaper, SANS Institute. http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113.

[xxii] Worland, Justin. 2014. How That Massive Celebrity Hack Might Have Happened. September 1. Accessed September 17, 2014. http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/.

[xxiii] Beechey, Jim. 2014. "Using the Critical Security Controls to Measure and Fund Your Program." www.counciloncybersecurity.org. September 2. Accessed September 17, 2014. http://www.counciloncybersecurity.org/articles/using-the-critical-security-controls-to-measure-and-fund-your-program/.

[xxiv]Hoemeyer, Jane; Maxson, Margaret;. 2011. "Introduction to NICE Cybersecurity Workforce Framework." http://csrc.nist.gov/. September 20. Accessed October 6, 2014. http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Wednesday/Wed_Intro-Framework_Maxson_Homeyer_Mills.pdf.

Council on CyberSecurity

Le Conseil de la CyberSécurité