Senior Cyber Leadership: Why a Technically Competent Cyber Workforce Is Not Enough

www.csfi.us

TABLE OF CONTENTS

EXECUTIVE SUMMARY

There is no shortage of articles, news reports, white papers, policy reviews, congressional testimonies, and other sources describing cyber threats and their potential consequences to U.S. and international security. Given the international threat posed by activities such as cyber espionage, cybercrime and the potential for cyber attacks and cyber warfare, a generally accepted assessment exists that there is a critical shortage of skilled cybersecurity experts to mitigate and manage the cyber threat. This point is emphasized by the Center for Strategic and International Studies which has reported that there is a "desperate shortage of people who can design [adequately] secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts."

This report suggests that while significant and necessary emphasis has been placed on technical skills needed within the cyber workforce, little attention has been given to the people that will *lead* the future workforce. It is leadership that must develop sound strategy and manage adequately skilled resources to mitigate the cyber threat. This report focuses on the level of Senior Cyber Leadership and defines this as *someone who is responsible for enhancing the competitive advantage of an organization's mission and business processes and functions by innovatively leveraging resources, information and information technology to deliver solutions that are effective, efficient, and secure.*

This report analyzed thirty-two senior cyber leader position descriptions across seven critical sectors to assess the current "state of practice" for the knowledge, skills, and abilities organizations are seeking in their Senior Cyber Leader candidates. Based on this assessment, this report identified four competency areas: Leadership, C-level/Executive Management, Interdisciplinary, and Cyber-centered. A number of KSAs were identified within each competency. The research team then compared the results to three targets: existing cyber leader-related graduate programs, the National Institute for Standards and Technology National Initiative for Cyber Education Cybersecurity Workforce Framework, and two popular commercial certification regimens. The final outcome was a list of general key findings and observations as well as specific key findings and observations for each target.

General Findings and Observations

1. Senior Cyber Leaders must be able to effectively communicate cyber-related business cases and return on investment, oftentimes relying on persuasion and negotiation in a contested, complex business environment where the desire for more capability can trump the necessity for security.
2. Senior Cyber Leaders must remain technically competent, relying on a regimen of lifelong learning and leadership of technical studies and analyses. Commercial certifications serve as a firm foundation for the growth of future Senior Cyber Leaders.
3. Senior Cyber Leaders must pursue continuing leadership and management professional education. Being technically competent is not sufficient to contribute in C-level/Executive Management positions.

4. Senior Cyber Leaders do not have to follow a "cookie cutter" development path. Corporate culture is a critical factor in defining how experience, aptitude, and expertise are valued and prioritized in the hiring and placement process when selecting Senior Cyber Leaders.
5. Senior Cyber Leaders are difficult to find. Leadership skills are not emphasized in entry and mid-level cyber positions resulting in a sparse candidate pool for more senior cyber positions within organizations.
6. Senior Cyber Leaders should be the primary lead for the organization's Enterprise Architecture and a key team member of the organization's Risk Executive function.
7. There currently is no generally accepted set of cybersecurity performance metrics and evaluation criteria for Senior Cyber Leaders.
8. Senior Cyber Leader candidates do not necessarily have a standard minimum level of documented, relevant experience. It is not the intent of this report to specify experience requirements. However, assessing a candidate's experience against the competencies presented in this report can aid the human resources department and/or hiring authority in making a hiring recommendation or decision.
9. Senior Cyber Leaders require organizational leadership and executive management support to be able to effectively carry out their responsibilities. Shifting the Senior Cyber Leader from an executive support role to a key member of the governance board will enable this change.
10. Expectations for a Senior Cyber Leader differ, sometimes greatly, from one organization to the next. This can cause a lack of understanding and affect executive communications. This in turn affects the organization's ability to effectively coordinate critical cyber activities such as timely and effective response to cyber threats within and across sectors.

National Cybersecurity Workforce Framework Findings and Observations

1. The National Cybersecurity Workforce Framework states that it "classifies the typical duties and skill requirements of cybersecurity ***workers***" (emphasis added.) It appears to define the technical skills and competencies required of cybersecurity practitioners yet it does not identify a workforce development framework nor does it address the special skills required of cyber leaders at all levels.
2. Of the 18 Knowledge, Skills, and Abilities (KSAs) specified in the Strategic Planning and Policy Development category of the Oversight and Development Specialty Area, only one (Knowledge of the organization's core business/mission processes) is a non-technically-oriented skill. It maps to the Organizational Awareness competency, which merely defines that the individual must have "knowledge of the organization's core business/mission processes." There is no specification as to the depth and level of expertise associated with the concept of "knowledge" in the framework.
3. Leadership and managerial skills are not specifically identified as KSAs. In fact, they are noticeably absent in the Framework Specialty Areas describing both Information Systems Security Operations (Information Systems Security Officer) and Security Program Management (Chief Information Security Officer).
4. The "Oversight and Development" category was titled "Support" under a previous framework version. The shift to "Oversight and Development" is a welcome change,

however the framework does not go far enough to include leadership and management related KSAs.

Commercial Certification Organization Findings and Observations

1. CISSP and CISM are competencies found in most Senior Cyber Leader position descriptions.
2. No CISSP domains were assessed for membership in the Leadership or C-level/Executive Management competency bins. Given this certification is traditionally associated with mid-level management, this is not a shortfall per se. However, as professionals progress in the cyber leader careers, (ISC)2 should evaluate its Continuing Professional Education (CPE) program to include leadership and management related offerings to encourage non-technical professional development.
3. Although some may question the validity of "certifying" leadership, relying perhaps more on documented experience as a basis for assessment, a formal method for assessing lifelong learning and continued professional development focused on leadership and management KSAs would be beneficial for the technically-inclined cyber workforce.

Graduate Program Findings and Observations

1. "Mashups" between the engineering and business schools provide an excellent method to develop the leadership and technical KSAs essential for effective Senior Cyber Leadership.
2. Cyber leadership programs need to provide enough flexibility to account for executives with little or no previous technical education and experience (i.e., developing "cyber aware" leaders) as well as technologists that aspire to access C-level and executive management positions within their organizations.
3. More cyber leadership programs are needed to address the critical shortfall of cyber leaders in the burgeoning cybersecurity workforce.

INTRODUCTION

"Cyber defense requires not only IT experts with computer science, electrical engineering, and software security skills, but also professionals with an understanding of political theory, institutional theory, behavioral psychology, ethics, international law, international relations, and additional social sciences...the pillars of our society...are often led by individuals with extremely limited exposure to cyber issues and the existential threats they pose…"

Ms. Francesca Spidalieri
Fellow at the Pell Center for International Relations and Public Policy

There is no shortage of articles, news reports, white papers, policy reviews, congressional testimonies, and other sources describing cyber threats and their potential consequences to U.S. and international security. James Clapper, Director of National Intelligence, testified before the U.S. Congress early in 2013 that the cyber threat had surpassed terrorism as the highest threat to U.S. national security. U.S. Army General Keith Alexander, dual-hatted as the director of the National Security Agency and Commander of the U.S. Cyber Command, described the loss of industrial information and intellectual property via cyber espionage and cybercrime as the "greatest transfer of wealth in the history of mankind." Former U.S. Secretary of Defense Leon Panetta warned of a potential "Cyber Pearl Harbor" that may result due to the insecurity of our national critical infrastructures. These calls, in part, led U.S. President Barack Obama to issue Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," and Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," in February of 2013 to drive cyber policy at the national level.

Cyber threats are not simply a problem for the United States, but for the international community as well. For example, Estonian President Toomas Hendrik Ilves noted at the 2012 International Conference on Cyber Conflict that "the physical and the cyber worlds are quickly converging and boundaries between the "cyber" and the "real" world have begun to disappear. This, in turn, implies a convergence between cybersecurity and overall global security." President Ilves perhaps is uniquely qualified to discuss cybersecurity since his country is well-known for mitigating a 2007 cyber attack which was the first cyber incident recognized as impacting an entire nation-state.

Given the international threat posed by activities such as cyber espionage, cybercrime and the potential for cyber attacks and cyber warfare, a generally accepted assessment exists that there is a critical shortage of skilled cybersecurity experts to mitigate and manage the cyber threat. The Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency report, "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters," stated that there is a "desperate shortage of people who can design [adequately] secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts."

The technical skills called out by CSIS are echoed by the educational standards the National Security Agency (NSA) has established for an educational institution to earn the NSA Center of Academic Excellence in Information Assurance Education (CAE/IAE) designation. As a result of the emphasis placed on highly specialized, technical skills, cybersecurity-related curricula are predominantly taught in the computer science and engineering schools at most universities. Similar efforts exist internationally, including Great Britain's "Academic Centres of Excellence in Cybersecurity" program and the work of international cybersecurity firms like Kaspersky labs sponsoring yearly international cybersecurity student competitions.

This report suggests that while significant and necessary emphasis has been placed on technical skills needed within the cyber workforce, little attention has been given to the people that will *lead* the future workforce. There are those that view cyber threat through the lens of national security risk and the potential for a "Cyber Pearl Harbor", or business risk and the potential loss of intellectual property and competitive advantage. Regardless of one's view, it is leadership that must develop sound strategy and manage adequately skilled resources to mitigate the cyber threat. As Jason Healey, Director of Cyber Statecraft of the Atlantic Council, notes in his book A Fierce Domain: Conflict in Cyberspace from 1986 to 2012, a number of cyber events serve as "wake up calls" to expose potential cyberspace threats, yet similar occurrences repeat. This is a failure of leadership.

As academia, organizations, and nations seek to develop a future generation of technically proficient cybersecurity specialists, a number of questions readily come to mind:

- Who will lead this future cyber workforce in the furtherance of the organization's mission and business strategies?
- What knowledge, skills, and abilities (KSAs) are essential for these cyber leaders?
- Are these KSAs currently being taught in colleges and universities? In the private and public sectors? Are they required by commercial certifying organizations?

Regarding U.S. colleges and universities, a report by the Pell Center's Francesca Spidalieri assessed the top graduate schools in a number of interdisciplinary areas, including business administration, public policy, health care management, and other non-technical fields to determine if any of these programs offer electives, concentrations or other opportunities for their students to learn about cyber threats, vulnerabilities, and consequences. Her research concluded that cyberspace and cybersecurity education remains lacking and underdeveloped in most of the top-rated schools in the U.S. A handful of schools such as George Washington University, George Mason University, Washington University of St. Louis, and the University of Washington, however, have recently developed "Cyber Leader" graduate programs that are mash-ups of their Engineering and Business Schools. On the public sector side, the U.S. Department of Defense's National Defense University Information Resources Management College also offers a "Cyber Leader" graduate concentration under their Government Information Leadership graduate program. The key is whether or not these programs are teaching the appropriate KSAs in light of current and future cyber threats, a point this report addresses later.

The National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) is representative of the public sector's attempt to address cyber-related educational requirements. The NICE framework identifies seven categories of which six are specific cyber specialties. The seventh category, "Oversight and Development," does address some of the KSAs expected by such organizational positions as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). This report investigates whether or not these KSAs are sufficient in light of the growing cyber threat.

In addition to formal education, commercial certifications are very often key discriminators by which many private and public sector organizations have assessed applicants and employees for advancement. For example, the private sector has adopted the International Information Systems Security Certification Consortium's (ISC)2 Certified Information Systems Security Professional (CISSP) as the de facto standard for cybersecurity managers. In fact, one senior executive interviewed for this report said that if an applicant seeking employment with her company has a bachelor's or a master's degree, but does not have a CISSP, the human resources department will not forward his/her resume for consideration. There are other examples of organizations where a Master's of Science in IT Security may supersede the requirement of holding a CISSP. This reliance on commercial certifications begs yet another question: "Does a CISSP-like certification provide the sufficient KSAs for someone in a cyber leadership role or should there is something beyond a CISSP?" The CSIS report previously referenced addresses this question by stating that the "current certification regime is not merely inadequate, it creates a dangerously false sense of security…" The National Academy of Sciences recent report, "Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making," concludes that the cybersecurity field is still young and the "technologies, threats, and actions taken to counter the threats that characterize the endeavor are changing too rapidly to risk imposing the rigidities that typically attend professional status." Whether one agrees or disagrees with these assertions, it is clear that an organization's Senior Cyber Leadership is essential in navigating these critical workforce issues.

SENIOR CYBER LEADERSHIP

"Because cybersecurity is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cybersecurity workforce."

Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making
National Academy of Sciences

Although cyber leadership is required at all levels in an organization, it is the senior "C-suite" cyber executive leader and corresponding executive management who lead and manage the highly skilled cyber workforce to advance the organization's mission and business strategies. Just as the traditional C-suite executive credentials include MBAs, CPAs, Juris Doctorates, and other specialized higher education degrees, Senior Cyber Leaders should be expected to hold similar standards in order to maintain the trust and confidence of their peers and the cyber workforce at large. This report describes what KSAs should be expected from a Senior Cyber

Leader in order to assist universities, commercial certification organizations, and the public and private sectors in order to develop future Senior Cyber Leaders desperately needed to mitigate growing cyber threats.

This report defines a Senior Cyber Leader as *someone who is responsible for enhancing the competitive advantage of an organization's mission and business processes and functions by innovatively leveraging resources, information and information technology to deliver solutions that are effective, efficient, and secure.*

It is important to draw a distinction between the use of the words "cyber" in this report and "cybersecurity" in this report. While the term "cyber" was chosen to reflect the role of an executive with broader information, technology, and security responsibilities, the term "cybersecurity" is traditionally associated with the role of a Chief Information Security Officer (CISO) or equivalent. Currently, much of the existing literature does not make this distinction. This report asserts that Senior Cyber Leaders must develop a broader, multi-disciplinary set of skills.

Based on our analysis and research, this study categorizes KSAs into four separate segments that a Senior Cyber Leader should master to achieve this definitional standard: Leadership, C-Level/Executive Management, Interdisciplinary, and Cyber-Centered.

Leadership is the primary responsibility of a Senior Cyber Leader and is the foundation that sets a Senior Cyber Leader from the technical expectations usually associated with cyber. These are the so-called "soft skills" required of most senior organizational leaders.

C-Level/Executive Management competencies are needed to effectively interact with the board of directors, C-level executives, executive management, and other stakeholders in order to affect the strategic direction of the organization.

Interdisciplinary competencies are needed to support C-level executives and executive management in decision-making affecting one or more missions, business functions, or processes within the organization or in support of a corporate, board-level, or equivalent decision.

Cyber-centered competencies are needed to provide the greatest *technical* insight and decision making support to the organization. This category sets a Senior Cyber Leader apart from other peers in the board room. These are the competencies centered on the information and information technology aspects of an organization and those that make the Senior Cyber Leader the "technical authority" on the executive team.

This study attempts to illuminate the level of technical skill required at the most senior levels of cyber-related responsibilities. Furthermore, given the dynamic nature of cyberspace, a Senior Cyber Leader should demonstrate a lifelong commitment to continuous professional development in order to leverage current and emerging technologies to achieve their organization's strategic objectives.

Although this report focuses on Senior Cyber Leader KSAs, it is incumbent on all organizational senior executives to be "*cyber aware*." This can be achieved by developing the Cyber-centered KSAs. This segment is particularly helpful for non-technical senior executives who need to understand the impact of potential cyber threats to their organization.

It is not the intent of this report to redefine the roles of the CIO, CISO, or other C-suite executive positions. Nor is its intent to prescribe a singular organizational structure. Each organization is defined by its culture, size, sector, resources, risk tolerance, and so on. No single solution will fit all organizations. Instead, this report defines Senior Cyber Leadership and the KSAs required in an organization's executive team. Whether these KSAs are inherent in one executive position or incorporated into a number of executive positions, research indicates that they should be present at the C-suite level in order to counter and mitigate the cyber threats that may otherwise reduce an organization's competitive advantage.

METHODOLOGY

The research for this report comprised several different phases. An initial brainstorming exercise included over 60 U.S. and international experts from a broad range of public and private sectors. A thorough literature review identified key sources related to major aspects of information technology, cybersecurity, privacy, risk/threat, and other relevant domains.

The literature review served as the basis for assessing the current state of proposed Senior Cyber Leader competencies. The competencies were then analyzed to determine logical groupings. These "bins" proved helpful in further illuminating the distinctions between "cyber aware" leaders and "cyber leaders."

The next step involved assessing the present "state of practice" in terms of the position requirements that are currently advertised for various Senior Cyber Leadership positions, including Chief Information Officers (CIO), Chief Information Security Officers (CISO), Chief Threat Officers, Chief Risk Officers, and executive management positions supporting the C-Level. Target sectors were identified based on the U.S. Department of Homeland Security's listing of national critical infrastructures. To further scope the project, these target sectors were filtered based on cybersecurity industry threat reporting to select the most "at risk" sectors.

Project members conducted a congruence analysis of position descriptions for each sector, identifying keywords and concepts related to Senior Cyber Leadership. The bins developed from the previous step were used to organize the keywords and concepts. Project members then assessed the results of each sector and synthesized a general, sector-specific competency description. This analysis and synthesis also served as a cross-check to ensure the bins were comprehensive and complete.

TARGET SECTOR ANALYSIS

In conducting research for this report, the group considered the critical infrastructures identified by the U.S. Department of Homeland Security. Seven sectors were selected for

detailed study: government, intelligence, energy, telecommunications, finance, health care, and transportation. The analysis of these sectors can serve as a baseline from which other sectors can model their Senior Cyber Leader requirements.

Thirty-two position descriptions were analyzed with a minimum of three position descriptions per sector. The project team experienced a number of difficulties attaining position descriptions representative of Senior Cyber Leader positions. First, some positions did not have formal, detailed descriptions or they were not publicly available. Second, positions descriptions are often out of date and do not reflect the incumbents' actual responsibilities. Finally, a number of organizations did not appear to have C-suite or executive management positions that met this project's Senior Cyber Leader definition. This may reflect, among other reasons, a lack of awareness as to the benefit of having a "cyber-minded" organizational executive. Despite these difficulties, the project team was successful in selecting a representative sample of position descriptions to conduct its research.

The majority of position descriptions required a minimum of a Bachelor's degree, usually in a technical discipline such as computer science, engineering, mathematics and the like. A majority also highly desired advanced degrees, including business, policy, public administration, as well as technical disciplines. Likewise, the majority required commercial certifications including: CISSP, Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC) Information Security Professional (GISP), Information Technology Infrastructure Library (ITIL) and other similar certifications.

The following sections present the generalized description of expected KSAs across all seven sectors organized by the previously described groupings: Leadership, C-Level/Executive Management, Interdisciplinary, and Cyber-centered.

Leadership

As the term implies, Senior Cyber Leadership is first and foremost a leadership issue. The KSAs associated with this bin are what professionals generally consider the "soft skills" executives must possess and effectively employ in order to successfully drive their organization's strategy. Given the breadth and depth of leadership studies available, this study does not attempt to address the concept of leadership in detail. Instead, it is worth noting the traits common to many of the sectors and Senior Cyber Leader positions analyzed.

The most commonly identified Senior Cyber Leadership trait was the ability to effectively communicate complex technical matters in a manner that other senior leaders can understand. Cybersecurity is primarily about risk management and Senior Cyber Leaders must be able to articulate their observations and recommendations within the context of the organization's risk management program. Along these lines, they must be able to champion their cause in a potentially contested, resource constrained environment. Key skills such as influence, persuasion, and negotiation are necessary in these instances. They must be comfortable with

complexity. This is especially true as Senior Cyber Leaders are regularly called upon to lead cross-functional business and technical teams.

Like all leaders, a Senior Cyber Leader must take initiative, motivate, exhibit creativity and innovation, and provide sound, seasoned judgment. Mentoring and professional development round out the key leadership traits for Senior Cyber Leaders.

C-Level/Executive Management Competencies

As a C-Level or executive manager, many position descriptions strongly emphasized a Senior Cyber Leader's need to develop high-level networks and relationships within and outside an organization to solve complex, unyielding, unprecedented, and sometimes controversial challenges. Skills needed include the ability to advise, liaise, represent, interact, and advocate. Common relationships targeted senior executives in the interagency, private, and international sectors, as well as political leaders and staffs. These relationships form the basis for developing sound situational awareness and can lead to formal strategies for information exchange and cyber threat intelligence sharing.

All positions also required an in-depth understanding of the organization's strategy, policies, mission, and business objectives usually in the context of strategic planning, operational risk, and applicable federal laws, regulations, statutes, and other governing frameworks.

Although not applicable to all mission and/or business domains, in organizations that possess trade secrets, intellectual property, confidential research and development information, and similar sensitive information, the Senior Cyber Leader is an essential team leader in ensuring these assets remain secure.

Interdisciplinary Competencies

The majority of position descriptions identified knowledge of other essential organizational functions and disciplines as a critical enabler for success. These include:

- Enterprise Architecture
- Portfolio/Program Management
- Risk Management
- Delivery Assurance
- Business Analysis
- Budgeting and Finance
- Contracting and Acquisition
- Human Resources
- Cost-benefit Analysis and Return on Investment (ROI)
- Organizational Effectiveness and Continuity
- Continuous Improvement
- Disaster Recovery and Continuity
- Sector-specific legal, statutory, and regulatory requirements and organizations

- Export controls
- Antitrust laws
- Business Intelligence (BI)

Again, the ability to prepare and present highly complex technical issues at the executive-level in a manner understandable by non-technical personnel is expected. At the interdisciplinary level, Senior Cyber Leaders would assist in translating business requirements into technical solutions as well as resolving technical problems in the context of the organization's business model. This leads, in part, to establishing the proper balance between operational necessity and information technology expenditures and systems security.

Cyber-Centered Competencies

At its foundation, this category requires the fundamental competency of a Senior Cyber Leader to be able to extensively prepare or already be familiar with complex contemporary technical subject matter. This enables the Senior Cyber Leader to be adept at leading endeavors such as Enterprise IT and Security Architectures. This should not be confused with the broader Enterprise Architecture competency highlighted in the previous section.

All position descriptions listed the following cyber-centered competencies:

- Enterprise design, development, integration and interoperability, capacity planning, engineering, operations, and maintenance
- Information Security/Information Assurance
- Vulnerability Assessment
- Systems Life-cycle Management
- Performance Management
- Test, evaluation, and review of technical baselines
- Certification and Accreditation
- Vendor Management
- Computer, software, and database development
- Operating systems
- Cryptographic principles
- Voice, data, video, and imagery transport
- Network management and security
- Lead high-level research and technical studies
- Determine applicability, suitability, and effectiveness of new/emerging IT
- Public and private sector best-practices
- Cybersecurity strategy
- Data analytics
- Cyber terrorism strategy
- Cybersecurity governance related to the organization's mission and/or business domain
- Cybersecurity policy development and oversight
- Coordination and review of cyber-intelligence sharing
- Data loss prevention

- Knowledge of U.S. and International standards such as FISMA, NIST, and ISO 27000 series, COBIT
- Hacker methodologies and tactics
- Knowledge of key indicators of attacks and exploits
- Active involvement with fraud and security penetration
- Designing appropriate Fraud and Security Systems

NIST NICE CYBERSECURITY WORKFORCE FRAMEWORK OVERVIEW

Analysis of the Senior Cyber Leader position descriptions showed that organizations across sectors had significant breadth and depth in the cyber KSAs expected of Senior Cyber Leader candidates. The NIST NICE National Cybersecurity Workforce Framework is a public sector attempt to codify the key tasks and KSAs recommended for a number of cyber-related specialties.

The framework consists of seven categories: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze, Oversight and Development. Each category is further subdivided into specialty areas. Each specialty area has a description, related job titles, key tasks, and recommended KSAs. The framework is a comprehensive document spanning a total of 31 cybersecurity specialty areas.

The Oversight and Development category is most relevant to this report as it contains "specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work." This category contains five specialty areas: Education and Training, Information Systems Security Operations, Legal Advice and Advocacy, Strategic Planning and Policy Development, and Security Program Management. Whereas the other framework categories and specialty areas fit squarely within the context of the cyber-centered competency bin, this category expands the framework's reach into the interdisciplinary and C-level/executive management competency bins.

The Strategic Planning and Policy Development and Security Program Management specialty areas most closely resemble the KSAs identified during the position description analysis. The former specialty area "applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest; develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements." Related job titles include CIO and Policy Writer and Strategist. The Security Program Management specialty area "manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources." Related job titles include CISO and Risk Executive.

GRADUATE EDUCATION PROGRAM OVERVIEW

Analysis of the Senior Cyber Leader position descriptions showed that organizations across sectors required or highly preferred advanced, technical degrees. A smaller portion addressed advanced degrees directed toward business, policy, and similar degrees. There is a growing trend among graduate schools to offer "Cyber Leader" related degrees. The programs highlighted in this report are not intended to be all-inclusive, but they do reflect the most commonly searched on Google using the search string "Cyber Leader." Given this trend, it is instructional to briefly highlight some of these graduate programs as a precursor for further discussion later in the report. Each program discussed below includes a narrative description as well as a mapping of each program's course requirements to this projects Senior Cyber Leader competencies.

1. George Mason University (GMU) offers a graduate degree in Management of Secure Information Systems, described by GMU as a "cross-disciplinary cybersecurity degree program." It is a mashup of the School of Management, School of Public Policy, and Volgenau School of Engineering that emphasizes strategic leadership, decision making, business fundamentals, and technical studies. GMU targets mid-career professionals and the program is accredited by the NSA and DHS as a National Center of Academic Excellence in Information Assurance Education and a National Center of Academic Excellence in Information Assurance Research.

Leadership	**C-level/Executive Management**	**Interdisciplinary**	**Cyber-Centered**
● Communications and Leadership	● Mgmt of Consulting and Technology Professionals ● Economics of Technical Mgmt ● Organizations, Mgmt, and Work: Theory and Practice ● Decision Making Using Accounting and Finance Data	● Security Practices in the Enterprise ● Secure Information Systems Governance, Risk, Compliance ● Privacy and Ethics in an Interconnected World	● Foundations of Cybersecurity ● Networking Principles ● Networking Security ● Enterprise Security Threats ● Technology Assessment, Evaluation, and Investment ● Enterprise Security Technology ● Critical Infrastructure Protection in Theory, Policy, and Practice

2. The George Washington University (GWU) offers a World Executive MBA in Cybersecurity. It is a mashup of School of Business and the GWU Cyber Center for National and Economic Security (CCNES) and has the expressed goal to educate leaders in the "C-suite and in the trenches" to "meet and defeat cyber threats to global business in real-time." The curriculum includes accounting, finance, marketing, business ethics, decision-making, U.S. and global cybersecurity strategy, policy, partnerships, and law, "covering the full spectrum of threats." The program targets professionals from the National Security and Corporate/Finance sectors that operate in the nexus of business, technology, and security. These students are challenged to consider the "economic, cultural, social, and political realities" associated with cybersecurity.
3.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
• Judgment, Uncertainty, and Decisions • Organizations and Leadership	• Operations Strategy • Financial Markets • Global Perspectives • Microeconomics for the Global Economy • International Management • Nature of Markets • Marketing Decisions • Business and Public Policy • Business Law and Communication	• Managerial Accounting • Financial Accounting • Data Analysis and Decisions • Business Ethics • Managing Human Capital • Entrepreneurship • Business Strategy • Business Communications	• Cybersecurity Elective Area

4. The University of Maryland University College (UMUC) offers two cyber leadership graduate degree options: Cybersecurity and Cybersecurity Policy. Both programs target mid-career professionals employing a multi-disciplinary curriculum. The former includes coursework in management, law, science, business, technology and psychology, focusing on prevention, detection, countering and recovering from cyber incidents. The Cybersecurity Policy program includes coursework in human aspects in cyber security, national security policy and law, enterprise cyber security policy and global cyber security. As stated on the UMUC site, "The roles of government, inter-organizational alliances and international cooperatives are explored, as are such legal concepts as privacy, intellectual property and civil liberties." UMUC also has a dual-

degree option in which they pair these cybersecurity degrees with their MBA program. Note that the courses listed below are each six credits.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
• None	• National Cybersecurity Policy and Law • Global Cybersecurity	• Human Aspects in Cybersecurity: Ethics, Legal Issues, and Psychology • Enterprise Cybersecurity Policy • Cybersecurity Capstone	• Cyberspace and Cybersecurity

5. The University of Washington (UW) offers a graduate degree in Cybersecurity and Leadership. The program is a cooperative effort between UW's Center for Information Assurance and Cybersecurity and the Milgard School of Business' MBA program. The program provides "a thorough knowledge base for managers and technology leaders concerned with the design, development, implementation, operation, and management of cybersecurity systems, and the protection of an organization's information assets." With this knowledge, students are prepared to lead technology professionals and organizations to defend against cyber threats.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
• Organizational Change	• Strategic Management	• Business Ethics and Social Responsibility • Designing and Executing IA/Cybersecurity Strategies • Business Communications • Building an Information Risk Management Toolkit • Individual and Team Dynamics	• Principles of Cybersecurity • IA/Cybersecurity and Risk Management in Context • Network and Internet Security

6. The Washington University in St. Louis (WUSTL) offers a graduate degree in Cyber Security Management. The program is a cooperative effort between WUSTL's School of Engineering and Applied Science and the Olin Business School. All degree candidates must have over five years of demonstrated experience in the business or government sectors as a prerequisite for admission into the program. One-quarter of the curriculum requires coursework in business and organization and the electives portion offers additional opportunities for leadership and management coursework. The program "examines the impact that Information Security as a discipline and Cyber Security Management as a practicum have on enterprise tactical, ethical, cultural and strategic performance from a managerial and executive perspective." Note that all the courses below are not required for the degree. The curriculum is divided into three areas: focus courses (four required; denoted by an "F"), elective courses (four required; denoted by an "E"), and business and organization courses (three required; denoted by a "B").

Leadership	**C-level/Executive Management**	**Interdisciplinary**	**Cyber-Centered**
• Managing Power and Politics (E) • Negotiation (E) • Organizational Behavior (B)	• Art and Science of Risk Management (F) • Principles of Strategic Planning (E) • Seminar in Enterprise Transformation (E) • Executive Perspectives for Technical Professionals (E) • Strategic Management of Technology (E) • Advanced Application of Risk Management and Decision Analysis (E) • Financial Principles of the Company (B) • Ethical Issues in Managerial	• View from the Bridge: Leading an Information Security Team (F) • Security Risk Analysis (F) • Enterprise Network Security (F) • Perspectives on Innovation and Technology (F) • Operations Planning and Control (E) • Human Performance in Engineering (E) • Life Cycle Cost Analysis (E) • Economics of Technology (B)	• Systematic View of Cyber Security and Information Assurance (F) • Programming Concepts and Practice (E) • Applied Cyber Security Practices in Computer Forensics and Cyber Warfare (F) • Incidence Response and Information Warfare (F) • Cyber Counterespionage - Case Study Analysis (F) • Cyber Security Metrics (F)

	Decision Making (B) ● Law and Business Management (B) ● Strategic and Crisis Communications (B) ● Introduction to Management and Strategy (B) ● Effective Management Communications (B)		

7. The National Defense University's Information Resources Management College offers a Cyber-L graduate degree concentration in their Government Information Leadership graduate program. Unlike the private sector offerings, this program is not a combination of engineering and business, instead focusing on cyberspace issues affecting national and strategic level strategy and policies. The curriculum is designed to integrate the "behavioral, cultural, and national intelligence perspectives with legal, digital forensic, and technology aspects especially from a prospectus on civilization," by addressing cyber governance, privacy and civil liberties, national security, interagency collaboration, cyber workforce protection, global cyber commerce and technology.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
● Organizational Culture for Strategic Leaders ● Decision Making for Government Leaders	● Multi-Agency Information-Enabled Collaboration ● Cyberspace Strategies ● Cyber Law ● International Perspectives on Cyberspace ● National Intelligence and Cyber Policy	● Leading the Cyber Workforce ● Continuity of Operations ● Privacy Rights and Civil Liberties ● Strategies for Assuring Cyber Supply Chain Security	● Terrorism and Crime in Cyberspace ● Critical Information Systems Technologies ● Critical Information Infrastructure Protection

COMMERCIAL CERTIFICATION OVERVIEW

Analysis of the Senior Cyber Leader position descriptions showed that organizations across sectors required or highly preferred commercial certification. These certifications included: CISSP, Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC) Information Security Professional (GISP), Information Technology Infrastructure Library (ITIL) and other similar certifications.

The most commonly listed certification was the CISSP. It is instructive to compare the 12 domains in the context of the competency bins to assess the completeness and comprehensiveness of the CISSP domains in relation to Cyber Leadership.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
• None	• None	• Information Security and Risk Management • Physical and Environmental Security • Business Security and Disaster Recovery • Legal, Regulations, Compliance, and Investigations	• Access Control • Security Architecture and Design • Telecommunications and Network Security • Cryptography • Software Development Security • Security Operations

Although not called out specifically in any of the position descriptions analyzed in this study, SANS does offer a Global Security Leadership Certification (GSLC) which of all commercial certifications reviewed for this report is the only certification explicitly addressing KSAs that were assessed as belonging to the C-level/Executive Management competency bin.

Leadership	C-level/Executive Management	Interdisciplinary	Cyber-Centered
• NONE	• Managing IT Business and Program Growth in a Globalized	• Building a Security Awareness Program	• 802.11 • Access Control and Password Management

	Marketplace ● Security and Organizational Structure	● Business Situational Awareness ● Disaster Recovery / Contingency Planning ● Facilities and Physical Security ● Incident Handling and the Legal System ● Information Warfare ● Managerial Wisdom ● Managing Ethics ● Managing Intellectual Property ● Managing Legal Liability ● Managing Negotiations ● Managing Privacy ● Managing Security Policy ● Managing the Mission ● Managing the Procurement Process ● Managing the Total Cost of Ownership ● Project Management For Security Leaders ● Quality ● Risk Management and Auditing ● Safety ● Selling Security ● Vulnerability Management -	● Change Management and Security ● Computer and Network Addressing ● Cryptography Algorithms and Concepts ● Cryptography Applications, VPNs and IPSec ● Cryptography Fundamentals ● Defense-in-Depth ● Defensive OPSEC ● DNS ● Endpoint Security ● General Types of Cryptosystems ● Honeypots, Honeynets, Honeytokens, Tarpits ● Incident Handling Foundations ● IP Terminology and Concepts ● Logging ● Malicious Software ● Manager's Guide to Assessing Network Engineer ● Managing PDA Infrastructure ● Managing Software Security ● Managing Technical People ● Methods of Attack ● Offensive OPSEC ● Security Frameworks

		User View	• Steganography • The Intelligent Network • The Network Infrastructure • Vulnerability Management - Inside View • Vulnerability Management - Outside View • Web Communications and Security • Wireless Advantages and Bluetooth

KEY FINDINGS AND OBSERVATIONS

Based on analysis of thirty-two position descriptions representing seven sectors, a number of KSAs were identified and categorized in four competency bins: Leadership, C-level/Executive Management, Interdisciplinary, and Cyber-centered. Overviews of the NIST NICE "Organizing and Developing" category, cyber-related graduate education programs, and industry standard commercial certifications were provided as background in order to assess these competencies in the context of the position description analysis and the professional experience of the research team. The result is a list of general findings and observations as well as specific findings and observations for NIST, graduate institutions, and commercial certification organizations to consider as they evolve their future offerings.

General Findings and Observations

1. Senior Cyber Leaders must be able to effectively communicate cyber-related business cases and return on investment, oftentimes relying on persuasion and negotiation in a contested, complex business environment where the desire for more capability can trump the necessity for security.
2. Senior Cyber Leaders must remain technically competent, relying on a regimen of lifelong learning and leadership of technical studies and analyses. Commercial certifications serve as a firm foundation for the growth of future Senior Cyber Leaders.

3. Senior Cyber Leaders must pursue continuing leadership and management professional education. Being technically competent is not sufficient to contribute in C-level/Executive Management positions.
4. Senior Cyber Leaders do not have to follow a "cookie cutter" development path. Corporate culture is a critical factor in defining how experience, aptitude, and expertise are valued and prioritized in the hiring and placement process when selecting Senior Cyber Leaders.
5. Senior Cyber Leaders are difficult to find. Leadership skills are not emphasized in entry and mid-level cyber positions resulting in a sparse candidate pool for more senior cyber positions within organizations.
6. Senior Cyber Leaders should be the primary lead for the organization's Enterprise Architecture and a key team member of the organization's Risk Executive function.
7. There currently is no generally accepted set of cybersecurity performance metrics and evaluation criteria for Senior Cyber Leaders.
8. Senior Cyber Leader candidates do not necessarily have a standard minimum level of documented, relevant experience. It is not the intent of this report to specify experience requirements. However, assessing a candidate's experience against the competencies presented in this report can aid the human resources department and/or hiring authority in making a hiring recommendation or decision.
9. Senior Cyber Leaders require organizational leadership and executive management support to be able to effectively carry out their responsibilities. Shifting the Senior Cyber Leader from an executive support role to a key member of the governance board will enable this change.
10. Expectations for a Senior Cyber Leader differ, sometimes greatly, from one organization to the next. This can cause a lack of understanding and affect executive communications. This in turn affects the organization's ability to effectively coordinate critical cyber activities such as timely and effective response to cyber threats within and across sectors.

National Cybersecurity Workforce Framework Findings and Observations

1. The National Cybersecurity Workforce Framework states that it "classifies the typical duties and skill requirements of cybersecurity ***workers***" (emphasis added.) It appears to define the technical skills and competencies required of cybersecurity practitioners yet it does not identify a workforce development framework nor does it address the special skills required of cyber leaders at all levels.
2. Of the 18 Knowledge, Skills, and Abilities (KSAs) specified in the Strategic Planning and Policy Development category of the Oversight and Development Specialty Area, only one (Knowledge of the organization's core business/mission processes) is a non-technically-oriented skill. It maps to the Organizational Awareness competency, which merely defines that the individual must have "knowledge of the organization's core business/mission processes." There is no specification as to the depth and level of expertise associated with the concept of "knowledge" in the framework.
3. Leadership and managerial skills are not specifically identified as KSAs. In fact, they are noticeably absent in the Framework Specialty Areas describing both Information Systems

Security Operations (Information Systems Security Officer) and Security Program Management (Chief Information Security Officer).

4. The "Oversight and Development" category was titled "Support" under a previous framework version. The shift to "Oversight and Development" is a welcome change, however the framework does not go far enough to include leadership and management related KSAs.

Commercial Certification Organization Findings and Observations

1. CISSP and CISM are competencies found in most Senior Cyber Leader position descriptions.
2. No CISSP domains were assessed for membership in the Leadership or C-level/Executive Management competency bins. Given this certification is traditionally associated with mid-level management, this is not a shortfall per se. However, as professionals progress in the cyber leader careers, (ISC)2 should evaluate its Continuing Professional Education (CPE) program to include leadership and management related offerings to encourage non-technical professional development. Although the CISM certification was not assessed directly in this study, it would be instructive for the Information Systems and Audit Control Association (ISACA), the certifying organization for CISM, to evaluate its own continuing education program similarly.
3. Although some may question the validity of "certifying" leadership, relying perhaps more on documented experience as a basis for assessment, a formal method for assessing lifelong learning and continued professional development focused on leadership and management KSAs would be beneficial for the technically-inclined cyber workforce.

Graduate Program Findings and Observations

1. "Mashups" between the engineering and business schools provide an excellent method to develop the leadership and technical KSAs essential for effective Senior Cyber Leadership.
2. Cyber leadership programs need to provide enough flexibility to account for executives with little or no previous technical education and experience (i.e., developing "cyber aware" leaders) as well as technologists that aspire to access C-level and executive management positions within their organizations.
3. More cyber leadership programs are needed to address the critical shortfall of cyber leaders in the burgeoning cybersecurity workforce.

THE FUTURE OF CYBER LEADERSHIP

Given the increasing threat related to operating in cyberspace, significant emphasis has been placed on developing a technically astute cyber workforce. Unfortunately, this emphasis has been at the expense of discussions related to cyber leadership. This study addressed this shortcoming by providing a definition for Senior Cyber Leadership, identifying four competency areas and highlighting relevant KSAs based on analysis of senior cyber leader position descriptions across seven sectors. Key observations and findings related to the primary

mechanisms for developing future cyber leaders have been provided based on graduate education programs, commercial certifying organizations, and the NIST NICE National Cybersecurity Workforce Framework. This research was based on current workforce practices. The next question may well be what issues will likely be most relevant for Senior Cyber Leaders in the future as these issues will drive the evolution of senior cyber leader development.

This report concludes with the challenges we expect Senior Cyber Leaders will most likely face in the next 3, 5, and 10 years:

By 2016 (3 Years):

- Senior Cyber Leaders will be responsible for gathering and maintaining an ever-maturing set of strategic cyber metrics that will be used by the board and senior management team to drive decisions related to strategy, operational management, and acquisition.
- Organizations seeking to hire Senior Cyber Leadership positions such as Chief Information Officer and Chief Information Security Officer will make certifications such as CISSP and/or CISM a prerequisite for their candidates.
- Most colleges and universities will offer undergraduate and graduate degree programs in Cybersecurity. Cybersecurity will become an important required subject in many business and law schools.
- Government laws and regulations will continue to evolve, presenting the Senior Cyber Leader with an ever-changing set of compliance, reporting, and disclosure issues. Privacy issues will be at the top of the list of concerns.
- Credentialing organizations will explore awarding cybersecurity credentials in tiers based on demonstrated levels of experience and formal continuing education requirements. Basic, Advanced, and Master level tiers will be proposed.

By 2018 (5 Years):

- With the continued growth of an information-based economy, the demand for Senior Cyber Leaders who have both strong technical qualifications and business leadership skills will increase significantly. Chief Risk Officers and Chief Security Officers will be expected to have formal training in cybersecurity measures and hiring authorities will begin to make cybersecurity credentialing a prerequisite for these positions.
- Credentialing organizations will adopt new standards that will award cybersecurity credentials based on demonstrated levels of experience and formal continuing education. Basic, Advanced, and Master levels will be adopted.
- Advanced degree programs in Cybersecurity will be seen advancing into skills requirements as organizations seek to hire candidates for Senior Cyber Leaders such as CIO and CISO.
- Cybersecurity courses will be required in all business and law schools for their degree-granting programs.
- International professional organizations will reach agreement on basic standard cybersecurity metrics. National government standards organizations will remain in discussions to establish formal international standards for cybersecurity metrics,

nomenclature, and information sharing. A key sticking point will be mandatory disclosure of breaches across international borders.

- Public policy will be significantly affected by ever-increasing calls for legal protections of privacy and anonymity. Senior Cyber Leaders will be subject to litigation and increased regulatory oversight over issues arising from their custodianship of personal information.

By 2023 (10 Years):

- For information-based businesses, successful performance in Senior Cyber Leader positions, such as CIO and CISO, will be seen as necessary prerequisites to C-suite positions such as CEO, COO, and (in some cases) CFO.
- Advanced degrees in Cybersecurity will be a requirement for over 50% of Fortune 500 Companies' CIOs and CISOs. Over 35% of General Counsels will have formal education in cybersecurity at the undergraduate or graduate level. Over 10% of COOs and CFOs will have formal education in cybersecurity at the undergraduate or graduate level.
- Many law schools will offer a Masters of Laws program with a cybersecurity focus.
- International standards for cybersecurity metrics will be established.
- Privacy issues on the Internet will be one of the main issues in the upcoming 2024 U.S. elections. Senior Cyber Leaders will be called upon to field capabilities that continue to reduce the risk of inadvertent disclosure of privacy information.

ACKNOWLEDGMENTS

Senior Authors:

Sean C. G. Kern, Lt Col, USAF, Assistant Professor, National Defense University

Ken Peifer, Director, CISM, Cyber Strategy and Integration, CYFOR Technologies

Senior Advisor and Contributor:

Brig. General Gregory Touhill (ret.), USAF, CSFI Advisory Director, CISSP)

CSFI Senior Cyber Leader Writing Team: (in alphabetical order):

Doug Capellman, CISSP
Ed Covert, CISSP, PMP, CISM, CRISC, Lead Associate, Booz Allen Hamilton
Geoff Hancock, CISSP, CISA, PMP
Royce Holden, MBA-TM, CISSP, Director of IT, Greater Asheville Regional Airport Authority
Ajay Porous
Vishwas Rudramurthy, Assistant Professor, GITAM University
Arjun Singh, MBA, CISSP, CCNA, MCSE
Ragna M. Sveinsdottir, MSc - IT Security, Digital Security Risk Management Team Lead
Jeff Teo, Ph.D, A+, Network+, Security+ and Certified Ethical Hacker, Professor of Computer Information Systems & Director of Online Programs at Montreat College
George Valencia, Jr., CISSP, Infrastructure Systems Architect
Sameer Valiyani, CSDA, M. Eng., Software Consultant

Special thanks to the following reviewers:

Christine de Souza, Information Assurance Engineer at Lunarline, Inc, USAF Cyber Surety

The Cyber Security Forum Initiative (CSFI) is a non-profit organization headquartered in Omaha, NE and in Washington DC with a mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners." CSFI was born out of the collaboration of dozens of experts, and today CSFI is comprised of a large community of nearly 29,000 Cyber Security and Cyber Warfare professionals from the government, military, private sector, and academia. Our amazing members are the core of all of our activities, and it is for them that we are pushing forward our mission.