Identifying Information Technology (IT) and Cybersecurity Executives' Competencies to Support Comprehensive Cybersecurity Programs

Paul E. Wagner and William E. Mapp
University of Arizona, Tucson, Arizona, United States

paulewagner@arizona.edu
mapp@arizona.edu

Abstract: Information Technology (IT) and cybersecurity executives play a pivotal role in shaping the cybersecurity posture of an organization. Their ability to make informed decisions, allocate resources, and communicate effectively with cybersecurity professionals is paramount. Consequently, these executives must acquire the necessary competencies that encompass cybersecurity risk management, legal and regulatory compliance, and strategic planning combined with foundational business and technical competencies. An interdisciplinary approach bridging the gap between business, technical skills and strategic decision-making is crucial to navigate the ever-evolving and complex cybersecurity challenges facing organizations today. Failure to do so may result in catastrophic consequences for both individual enterprises and society. Further, the growing frequency and sophistication of cyber threats pose significant risks to organizations and individuals alike. To effectively counter these threats, it is imperative to not only develop cybersecurity talent but also to equip IT and cybersecurity executives with essential competencies in this domain. Equally important, is to identify the specific competencies and develop an approach to train or teach them. According to Burrell, Aridi, & Nobles (2018) there is an extremely urgent need of leadership development for cybersecurity and information technology professionals to prepare these professionals with the foundational skills to excel in leadership, management, and directing an enterprise-level program. This paper underscores the critical need for a comprehensive understanding of both Information Technology (IT) and cybersecurity executive competencies and cybersecurity executive development. Integrating these two aspects is critical to improve an organization's cybersecurity posture and ensure alignment between organizational objectives and cybersecurity strategies. The two must work in tandem to create a robust and resilient cybersecurity infrastructure. This paper provides an analysis of the current literature regarding IT/Cybersecurity roles and responsibilities, leadership competencies, and technical competencies of IT/Cybersecurity executives to identify the gaps in existing research. The authors propose a survey instrument to conduct a quantitative analysis to identify executives' beliefs as to how important it is to possess each administrative competency. The survey is part of a future research plan to identify and evaluate administrative and technical competencies of IT/Cybersecurity executive leaders.

Keywords: Cybersecurity, Executive Leadership Competencies, Workforce Development

1. Introduction

The current state of cybersecurity and its workforce present challenges for leadership. Despite 70% of security professionals stating that generative artificial intelligence (AI) positively impacts productivity, collaboration, and morale, nearly 46% believe this technology will increase the organization's vulnerability to attack and 85% attribute the rise of attacks over the last 12 months to attackers' use of generative AI (White, 2023). For example, threats evolve by leveraging generative AI models to create malware, develop sophisticated phishing attacks and deepfakes, or collecting and analyzing data to identify new avenues of attack (Terranova Security, 2023). Through AI and other advanced techniques adversaries are now able to pivot from initial access to lateral movement within 84 minutes (Kurtz, 2022). This requires defenders to follow the 1-10-60 rule which is to detect threats within the first minute, understanding the threats within 10 minutes, and appropriately responding within 60 minutes (Kurtz, 2022).

The increase in the number, frequency, and sophistication of attacks takes a toll on cyber defenders. This leads to high turnover of cybersecurity talent and cybersecurity leaders. Stressors include staffing and resource limitations, rising complexity of technology, fear of risk due to generative AI, escalation of cyber-attacks, compliance and regulatory pressures, fear of generative AI taking jobs, remote work challenges, and public scrutiny and reputation concerns which are expected to drive nearly 51% from the industry (White, 2023). This, coupled with the fact that organizations identify skills gaps, shortages of cybersecurity staff, and despite these shortages, some organizations are reducing their cybersecurity staff (Coker, 2023). Further exacerbating the issue is the overall cybersecurity workforce shortage. Cyber Seek (2024) estimates that there are over 570,000 cybersecurity job openings in the United States and ISC2 (2023) estimates that 4 million cybersecurity professionals are needed globally.

2. Research Design and Methodology

2.1 Methodology

The authors used a systematic literature review (SLR) technique to find relevant academic articles from 2015 to 2024. Relevant information was extracted from select articles to inform analysis and discussion. The steps involved in the SLR process include:

1. Define the research questions.
2. Determine the data sources and search process.
3. Inclusion and Exclusion Criteria.
4. Results of searching and data extraction.
5. Analysis and Discussion.

2.2 Research Questions

1. What are the roles and responsibilities for Information Technology (IT) or Cybersecurity Executives?
2. What are the leadership competencies of the executives responsible for running an organization specifically for Information Technology (IT) or Cybersecurity executives?
3. What are the technical competencies of the executives responsible for running an organization specifically for Information Technology (IT) or Cybersecurity executives?

2.3 Data Sources and Search Process

A variety of sources were used to identify sources for this research including Google Scholar, IEEE, Elsevier, EBSCO, Proquest, and other library resources. Additionally, current industry trend reports were analyzed to identify current and relevant statistics and evidence to support research objectives. Search terms included the following terms with IT or cybersecurity prepended: workforce, leadership competencies, technical competencies, roles and responsibilities, opportunities, threats, and challenges. The search limited results from 2015 to present.

2.4 Inclusion and Exclusion Criteria

The authors used a liberal inclusive set of search criteria. Full-text journal articles were used to identify and analyze roles and responsibilities, leadership competencies, and technical competencies for IT / Cybersecurity executives. Information from these articles was extrapolated for their potential use in developing the survey instrument. Editorials, trade journals, and other online resources were used to identify the latest data for cybersecurity statistics and trends. Articles were reviewed and broadly categorized into roles and responsibilities, leadership competencies, and technical competencies. Additionally, articles providing context for workforce and the current threat landscape were included. Articles outside these categories were excluded from the systematic literature review.

2.5 Search Results

Search results can be broadly categorized into roles and responsibilities, leadership competencies, and technical competencies. Some results span across these categories.

3. Literature Review

The literature review provides context used to identify gaps in research and develop the survey instrument. Each section aligns with the broad categories identified during the literature review; specifically, Leadership Roles and Responsibilities, Executive Leadership Competencies, and Executive Technical Competencies. Salient elements were used to develop the proposed survey instrument.

The role of IT and cybersecurity executive leaders has become increasingly pivotal in safeguarding organizations against rapidly evolving cyber threats. The responsibilities of these leaders extend beyond leadership and technical competencies to encompass strategic decision-making, risk management, and compliance adherence. This section outlines the multifaceted realm of IT and cybersecurity workforce roles and the specific roles held by IT and cybersecurity executives. Primary sources for this section included the National Institute of Science

and Technology's (NIST) Special Publication (SP) 800-181 and National Initiative for Cybersecurity Careers and Studies (NICCS) Cyber Career Pathways Tool.

This understanding of roles and responsibilities provides a foundation for identifying and understanding the related leadership (Section 3.2) and technical (Section 3.3) competencies needed to fulfill the identified roles and responsibilities. The primary Knowledge, Skills, Abilities, and Tasks aligned with the Executive Cyber Leadership role is outlined in Table 1.

3.1 IT / Cybersecurity Executive Leadership Roles and Responsibilities

NIST SP 800-181rev1, the Workforce Framework for Cybersecurity (National Initiatives for Cybersecurity Education (NICE) Framework), currently identifies:

- Categories (7) – high-level grouping of common cybersecurity functions (Figure 1)
- Specialty Areas (33) – distinct areas of cybersecurity work
- Work Roles (52) – detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSA); now known as Tasks, Skills, and Abilities (TKS), required to perform tasks in a work role (NICCS, 2023).

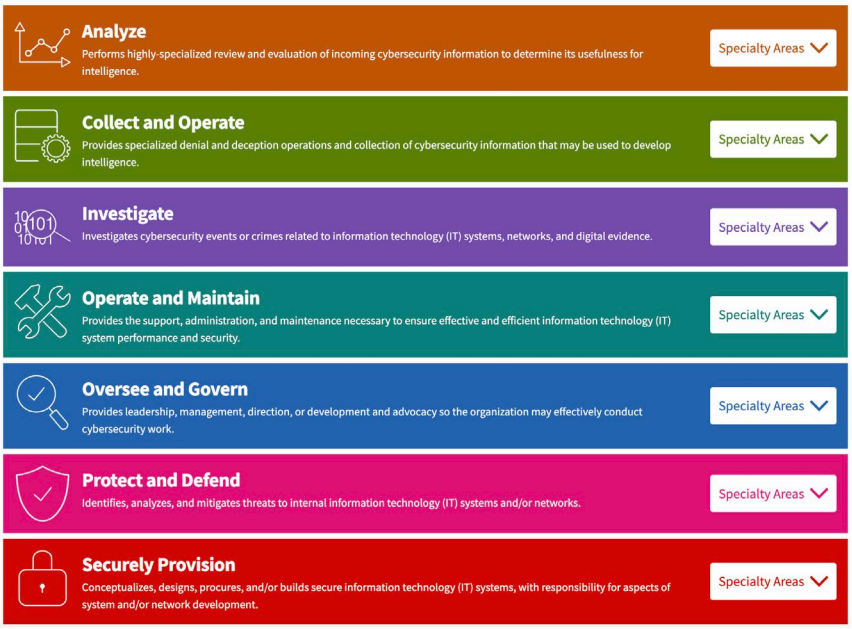

Figure 1: Workforce Framework Categories (NICCS, 2023).

Understanding these categories, specialty areas, and work roles provides organizations and executives the ability to develop effective cybersecurity teams. Additionally, analyzing the building blocks (Figure 2) for an effective cybersecurity workforce can prepare an organization. The circular arrows are activities which impact an organization, through the previously defined aspects of the NICE Framework, supported by the different pathways and experiences of the workforce which culminates in the capable and ready workforce (Newhouse, 2020).

Organizational complexity, the breadth of the information technology and cybersecurity field (Figure 2), growth of data, and reliance on technology both current and emerging have introduced multiple executive roles. These Chief-Suite or C-Suite positions may be directly related or corollary to IT and cybersecurity. The Chief Information Security Officer (CISO) and Chief Security Officer (CSO) roles are cybersecurity related positions. Chief Technology Officer (CTO), Chief Information Officer (CIO), and Chief Technology Innovation Officer (CTIO) are IT related positions. Corollary positions include Chief Compliance Officer (CCO), Chief Data Officer (CDO), and Chief Knowledge Officer (CKO). Executive Cyber Leadership is the work role within the Oversee and Govern category most applicable to this paper. Executive Cyber Leadership, "executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations." (NICCS, 2023).

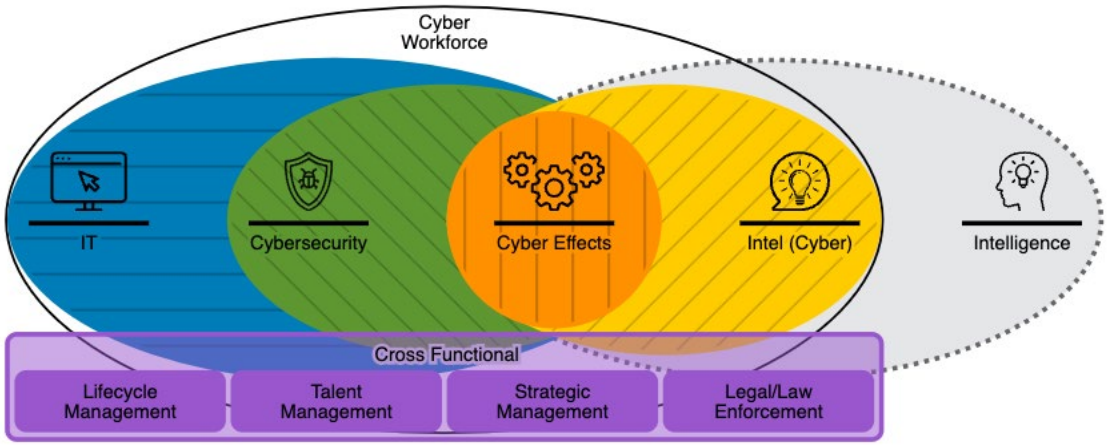

Figure 2: Cyber Career Pathways Tool (NICCS, 2023).

3.2 IT / Cybersecurity Executive Leadership Competencies

IT and Cybersecurity executive leadership competencies are consistent with leadership in other executive roles. Specific competencies can vary depending on the research. For example, Fotso (2021) compares traditional and emerging leadership theories. Their research identified human orientation, organizational skills, adaptability and flexibility, values, cognitive skills, self- awareness, transformational ability, and communication skills from traditional theories and sharing leadership style, handling complexity, knowledge, and global leadership from emerging theories (Fotso, 2021). Alternatively, Verlinden (2024) breaks down competencies into leading the organization, leading others, and leading yourself with associated competencies outlined in Figure 3.

Figure 3: Leadership Competencies (Verlinden, 2024).

The Workforce Framework further defines the Knowledge, Skills, Abilities, and Tasks (KSAT) for Executive Cyber Leadership summarized in Table 1. The Workforce Framework for Cybersecurity breaks Executive Cyber Leadership into entry level, 4-7 years of experience in a significant security role, intermediate 7-10 years of operational management experience, and advance, 10-15 years of high-level organizational and business strategy experience (NICCS, 2023). Additional capability indicators at each level include credentials and certifications, continuous learning, education, and training.

Table 1: Executive Cyber Leadership KSATs (NICCS, 2023).

Knowledge	Skills	Abilities	Tasks	
Computer networking and network security methodologies	Creating policies that reflect system security objectives	Develop policy, plans and strategy	Acquire and manage resources to support security goals and objectives to reduce organizational risk and conduct continuity of operations	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals
Risk management processes	Communicating with all levels of management	Apply critical thinking	Advise senior management on cost/benefit analysis of information security programs, policies, processes, systems, and elements	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies
Laws, regulations, policies, and ethics related to cybersecurity and privacy	Anticipate new security threats	Exercise judgement	Advocate organization's official position in legal and legislative proceedings	Identify security requirements specific to an IT system in all phases of the system life cycle
Cybersecurity and privacy principles	Remain aware of evolving technical infrastructures	Interpret and apply laws, regulations, policies, and guidance	Communicate the value of IT security throughout all levels of the organization	Ensure the plans of actions and milestones (POA&M) or remediation plans are in place for vulnerabilities identified during risk assessments, audits, and inspections
Cyber, System and Application threats and vulnerabilities	Use critical thinking to analyze organizational patterns and relationships	Tailor technical and planning information to a customer's level of understanding	Develop and maintain strategic plans	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate
Specific operational impacts of cybersecurity lapses		Prioritize and allocate resources	Interface with external organizations to ensure appropriate and accurate dissemination of incident and other Computer Network Defense (CND) information	Supervise and assign work to programmers, designers, technologies and technicians, and other engineering and scientific personnel
What constitutes a network attack and its relationship to both threats and vulnerabilities		Relate strategy, business, and technology in the context of organizational dynamics	Lead and align IT security priorities with the security strategy	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets
Emerging security issues, risks, and vulnerabilities		Understand technology, management, and leadership issues related to organizational processes	Lead and oversee information security budget, staffing, and contracting	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities
Capabilities, applications, and potential vulnerabilities of network equipment		Understand basic concepts and issues related to cyber and	Manage the publishing of CND guidance for the enterprise constituency	Design/integrate a cyber strategy that outlines the vision, mission, and goals

Knowledge	Skills	Abilities	Tasks	
		its organizational dynamics		that align with the organization's strategic plan
Industry technologies' potential cybersecurity vulnerabilities		Ensure information security management processes are integrated with strategic and operational planning processes	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards	Perform an information security risk assessment
Cyber competitions to develop skills		Ensure senior officials within the organization provide information security for the information systems that support operations	Recommend policy and coordinate review and approval	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities
			Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation
			Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals	Appoint and guide a team of IT security experts
				Collaborate with key stakeholders to establish a cybersecurity risk management program

3.3 IT/Cybersecurity Executive Technical Competencies

IT/Cybersecurity executive technical competencies are outlined in different research. Kappers and Harrell (2020) identify skills and certifications associated with different programming languages; enterprise architecture; firewall and intrusion detection/prevention protocols; knowledge of third-party auditing and cloud risk assessment methodologies; ISO 27003, ITIL and COBIT frameworks; network security architecture development and definition; various industry compliance assessments; secure coding, ethical hacking, and threat modeling; security architecture; TCP/IP, computer networking, routing, and switching; and various operating systems are requirements for employment at the CISO role. These are the like the knowledge areas outlined in Table 1. The required technical competencies can vary across industry sectors. Chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater are the 16 critical infrastructure sectors identified by the Cybersecurity & Infrastructure Security Agency (CISA) (CISA, 2024).

Despite identification of these competencies, the paths into the various IT/Cybersecurity C-Suite roles vary greatly depending on the path the executive took. Technical feeder roles include but are not limited to networking, software development, systems engineering, financial and risk analysis, security intelligence, and IT support. Potential pathways can be interactively mapped at a high level on Cyber Seek (Cyber Seek, 2024) or at a more granular level on NICCS (NICCS, 2023).

4. Gaps in Research

There is a gap in research on the specific IT/Cybersecurity executive leader's roles and responsibilities, leadership competencies, and technical competencies one should possess. As expressed by Burrell, Aridi, & Nobles (2018), there is an extremely urgent need of leadership development for cybersecurity and information technology

professionals to prepare these professionals with the foundational skills to excel in leadership, management, and directing an enterprise-level program, but there is not a lot of research addressing these topics. Researchers have been explicitly pointed to the need for such research and the fact that there is a gap in this area. For example, as stated by Cleveland and Cleveland (2018), "there is a gap between the level of knowledge regarding cybersecurity and the amount of information the executive leadership has in making informed decisions regarding cybersecurity"(p. 1).

The authors identified the following gaps in research based on the SLR.

1. The required depth or proficiency for technical competency at the C-suite level is not well understood. As IT/Cybersecurity professionals transition from entry-level through intermediate to advanced or C-Suite positions their level of technical competency may also shift. Additionally, the authors didn't identify studies which analyzed technical competencies of C-suite executives aligned with industry sectors. The training, education, and pathway to each sector could vary in terms of technical competency.
2. Various frameworks and leadership competencies were identified related to IT/Cybersecurity executives. Despite this, there are limited quantitative studies correlating these competencies and the level at which executives believe those competencies impact their position.

5. Future Research

As cyber-attacks, malware, and denial of service attacks on business and government entities become the norm and continue on a daily basis, the need for qualified IT/Cybersecurity professionals that have both technical and business skills continues to grow. As expressed by Burrell, Aridi, & Nobles (2018) when discussing the critical need for formal leadership training for cybersecurity and IT professionals, it is extremely important for them to possess the necessary leadership and management competencies to drive information security practices in today's enterprises. As a result, with the lack of research on leadership development programs for IT/Cybersecurity professionals, it is critical to find the necessary knowledge, skills, and abilities one should possess if they are, or aspire to be, a c-suite level professional. Once those competencies are identified, they can be added and implemented into a robust leadership program for IT/Cybersecurity professionals.

Understanding IT/Cybersecurity leadership and technical competencies is critical for several reasons. First, it can allow for developing curated training, education, and pathways to develop new professionals in this field to become competent executives in the future. Second, it can support organizations evaluate current professionals and develop their competencies or make more informed hiring decisions. Finally, professionals interested in achieving an IT/Cybersecurity C-suite position can better understand the requirements and plan their career path.

To that end, the authors will begin a two-phase mixed methods study to address these gaps in research. Phase one will focus on administrative competencies and phase two will focus on technical competencies. An initial survey instrument (*Leadership Competencies Instrument*) will be used to conduct a quantitative analysis to identify executives' beliefs as to how important it is to possess each administrative competency. The results will be analyzed, and participants will be asked to participate in interviews to provide qualitative data to provide additional context to the quantitative data. A corollary survey instrument will be developed focusing on technical competencies based on the literature review outlined in this paper and further review of updated literature. A similar round of interviews will be conducted to provide context and qualitative data.

The *Leadership Competencies Instrument* has been previously used on two separate research projects titled –*Leadership Competencies and their Development for Community College Administrators* and *Administrative Development for Academic Deans in the California State University System,* with an N=140 (201 Arizona community college administrators were surveyed, yielding a return rate of 69%); and N=40 (101 academic deans from 16 California institutions surveyed yielding a return rate of 39.6%) respectively. The theoretical perspectives used in survey instrument are grounded in the conceptual constructs associated with systems theory and Mintzberg's (1973) managerial roles. Mintzberg's (1973) framework examines managerial functions in the context of the daily work setting, concluding that a manager's work can be categorized into ten job roles, grouped into three categories: (1) interpersonal roles — figurehead, leader, and liaison; (2) informational roles — monitor, disseminator, and spokesperson; and (3) decisional roles — entrepreneur, disturbance handler, resource allocator, and negotiator (Grover & Jeong, 1993).

6. Conclusions

This paper provided an overview of the current state of cybersecurity threats and challenges to organizations and their leadership. This included pros and cons related to emerging technologies such as artificial intelligence, the speed at which attackers traverse organizational networks, and the overall sophistication of attacks. Additionally, organizations experience high turnover of cybersecurity talent due to various work related stressors. Further, organizations identify skills gaps, budgetary constraints resulting in layoffs, and overall workforce shortages within the field. These create a challenging environment for executives.

A systematic literature review was provided to identify existing research on the roles and responsibilities, leadership competencies, and technical competencies of IT and Cybersecurity executives. The review identified the Cybersecurity Workforce Framework that outlined the categories, specialty areas, and work roles. The paper further identified the different C-Suite roles related to IT and cybersecurity. The research then provided a comparison of traditional and emerging leadership theories which provided the specific leadership competencies and competencies related to leading the organization, leading others, and leading yourself. Further, The Workforce Framework for Cybersecurity outlined the specific KSATs associated with Executive Cyber Leadership. Finally, the framework's Knowledge and Skills identifies specific technical skills related to the executive cyber leadership role. These were like the competencies outlined by Kappers and Harrell.

Finally, the paper identified two major gaps in research. Despite research identifying the leadership and technical competencies, there is limited or no research that provides quantitative data on the level of proficiency required or how greatly these competencies impact current executives. Based on this, the authors proposed an initial survey instrument to identify the executives' beliefs as to how important it is to possess each administrative competency. Additionally, a brief research plan was discussed to further address these gaps.

References

Burrell, D. N., Ardi, A. S., and Nobles, C. (2018). The critical need for formal leadership development programs for cybersecurity and information technology professionals. *13th International Conference in Cyber Warfare and Security (ICCWS 2018).* https://www.proquest.com/openview/12cbf1c24ddb996f0f01a81fd12f4a4d/1?pq-origsite=gscholar&cbl=396500.

CISA (2024). Critical infrastructure sectors. *Cybersecurity & Infrastructure Security Agency (CISA).* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

Cleveland, S. and Cleveland, M., (2018, May). Toward cybersecurity leadership framework. In *Proceedings of the Thirteenth Midwest Association for Information Systems Conference*.

Coker, J. (2023, October 21). Cyber skills gap reaches 4 million, layoffs hit security teams. *Infosecurity Magazine.* *https://www.infosecurity-magazine.com/news/cyber-skills-gap-layoffs-security/*.

Cyber Seek (2024). Cybersecurity career pathway. *Cyber Seek.* https://www.cyberseek.org/pathway.html.

Cyber Seek (2024). Cybersecurity supply /demand heat map. *Cyber Seek.* https://www.cyberseek.org/heatmap.html.

Fotso, G. (2021, April 6). Leadership competencies for the 21st century: A Review from the Western World Literature. *Emerald Insight.* https://www.emerald.com/insight/2046-9012.htm.

Grover, V., Jeong, S., Kettinger, W. J., & Lee, C. C. (1993). The chief information officer: A study of managerial roles. *Journal of Management Information Systems,* 10(2), 107-130.

ISC2 (2023). ISC2 Cybersecurity Workforce Study. *International Information System Security Certification Consortium (ISC2).* *https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e*.

Kappers, W. and Harrell, M. (2020, June). From degree to Chief Information Security Officer (CISO): A framework for consideration. *Embry-Riddle Aeronautical University Scholarly Commons.* https://commons.erau.edu/publication/1575?utm_source=commons.erau.edu%2Fpublication%2F1575&utm_medium=PDF&utm_campaign=PDFCoverPages.

Kurtz, G. (2022). 2023 Global Threat Report. *Crowdstrike.* https://go.crowdstrike.com/2023-global-threat-report.html?utm_campaign=globalthreatreport&utm_content=crwd-treq-en-x-tct-us-psp-x-wht-brnd-x_x_x_x-reportsgtr&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%20threat%20report&gad_source=1&gclid=Cj0KCQiAtaOtBhCwARIsAN_x-3JHEysqJiG25w432wdl-JugGo0wZgmGBR5OF79_2XjsX6AyBUR3ZucaAvLbEALw_wcB.

Mintzberg, H. (1973). The Nature of Managerial Work. *New York. Harper and Row Publishers, Inc.*

Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2020, November 13). NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *National Institute for Science and Technology.* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf.

Mapp, W.E. (2007). *Leadership competencies and their development for community college administrators*. Walden University.

NICCS (2023, November 17). Cyber Career Pathways Tool. *National Initiative for Cybersecurity Careers and Studies.* https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool.

NICCS (2023, August 28). Executive Cyber Leadership. *National Initiative for Cybersecurity Careers and Studies.* https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/executive-cyber-leadership.

NICCS (2023, August 28). Workforce Framework for Cybersecurity (NICE Framework). *National Initiative for Cybersecurity Careers and Studies.* https://niccs.cisa.gov/workforce-development/nice-framework.

Terranova Security (2023). AI in cyber security: Pros and cons, and what it means for your business. *Fortra. https://terranovasecurity.com/blog/ai-in-cyber-security/.*

Verlinden, N. (2024). 18 Key leadership competencies for 2024 success. *Academy to Innovate HR (AIHR).* https://www.aihr.com/blog/leadership-competencies/.

White, A. and Bunce, J. (2023). Generative AI and cybersecurity: Bright future or business battleground? *Sapio Research. https://info.deepinstinct.com/voice-of-secops-v4-2023?_ga=2.86841240.1038042311.1705606129-1595372854.1705443616.*