

Brian Ho

7 May 2024

Soft Skill Nightmare: The Cybersecurity Skills Gap Necessitates an Emphasis on Critical Thinking

Introduction

The cybersecurity landscape is frequently portrayed by the media as facing a dire staffing crisis, with claims of up to 3.5 million positions remaining unfilled in 2023 (Morgan). However, an even more critical challenge is highlighted by the ISC2's Cybersecurity Workforce Study: the skills gap (ISC² 3). This gap, defined by the disparity between the skills cybersecurity professionals have and those employers deem necessary, is viewed by 59% of the workforce as a more significant issue than the staffing shortage (ISC² 22). Furthermore, 58% of respondents believe that the negative effects of the staffing shortage could be alleviated by addressing the skills gap (ISC² 6).

In a world where 71% of employers acknowledge that a shortage of skilled professionals cause measurable harm to their organizations (Crumpler 1), with cyberattack losses totalling \$10.3 billion in 2022 (FBI Internet Crime Complaint Center 3) and overall upward trend of cybercrime (Sharif 154), the importance of properly training the next generation of security professionals has never been greater.

A recent study analyzing the skills gap found that "It would be advantageous for educational programs to adapt their curricula and professional field experience programs to develop multiple training pathways that best prepare students and professionals for the varying position requirements within the sub-fields" (Ramezan 105). However, simply addressing

position requirements, such as the technical skills and industry certifications mentioned in the study, won't be enough. It is imperative that the cybersecurity industry pivots towards the development of critical thinking within its workforce. Emphasizing this soft skill in education, supported by business initiatives, is not merely beneficial but essential in developing a robust defense against increasingly sophisticated cyber threats. By fostering a workforce that is as adept in critical thinking as it is in technical know-how, the security community can better mitigate the complex security challenges of tomorrow.

Importance of Critical Thinking in Cybersecurity

The unpredictable nature of cyber threats, where attacks can occur at any moment and in unforeseen ways, underscores the necessity for blue teamers to possess critical thinking skills. Experts highlight, "Even if the timing and targets of the attacks were predictable, the types of technologies and techniques that could be brought to bear could be highly complex (novel and multifaceted), requiring creativity and critical thinking skills" (Schmidt 24).

The existence and prevalence of zero-day (previously unknown) attacks help further illustrate this necessity. According to a study by Ponemon Institute, "80 percent of respondents say the type of endpoint attack they experienced was a new or unknown zero-day attack" (Ponemon Institute LLC 4). Since zero-day attacks lack existing information and research, security professionals must apply critical thinking skills to identify novel anomalies in logs and synthesize their knowledge in mounting an effective response.

Bad actors may also implement defensive measures in their attacks, such as malware authors leveraging anti-debugging techniques in their code. "Functions associated with collect and operate and analyze are also driven strongly by external factors—namely, the characteristics

and actions of the targets. To be successful, these functions need to adapt to the potentially complex, layered, and unpredictable defensive measures taken by targets. This again requires creativity and critical thinking skills to outmaneuver the defense” (Schmidt 24).

Many security professionals tend to agree with the importance of critical thinking: For example, Richard Bejtlich, Security Strategist for Corelight, stated “Critical thinking is the single most important cybersecurity skill. Distilling a complex situation into its essential elements is key to mitigating digital challenges. Cybersecurity professionals must be able to observe the environment, challenge assumptions, create courses of action, and execute operations. Critical thinking enables each of these steps” (Tripwire Guest Authors). Similarly, 20 year FBI veteran Jill Knesek contributes, “In my opinion, the most critical skill for a cybersecurity professional is critical thinking ... For me, critical thinking is about understanding the ‘why’ and not just the ‘how’ so you can make good decisions and implement solutions that address the root cause of an issue and not just the symptom” (Tripwire Guest Authors).

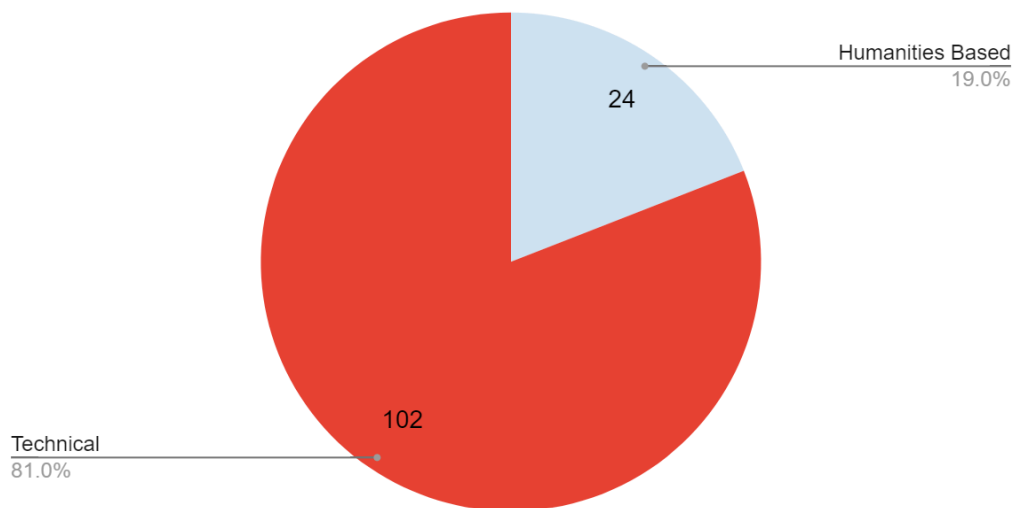
It’s important to clarify that this paper does not aim to entirely dismiss the need for technical skills in the industry. In fact, a study highlights that “the United States not only has a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design 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” (Crumpler 2). It is simply that “although there has been a strong focus in creating initiatives for technical skill development, soft skills such as communication and critical thinking are often pushed aside” (Weithers). Studies have found that such skills are not only the most critical in personnel, but that they are also the most difficult to find in an applicant, even over highly technical skills (Costanzo

12).

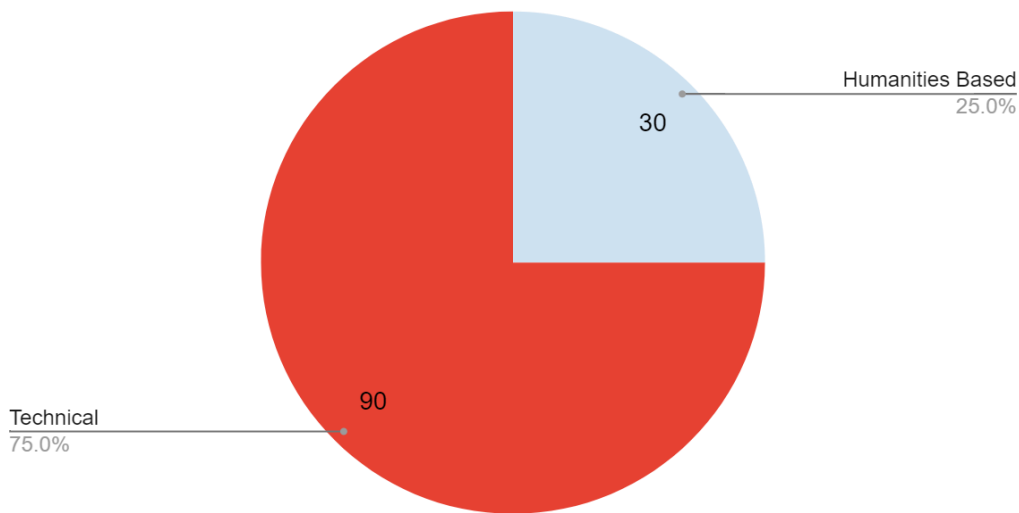
Challenges in Current Educational Models

Developing critical thinking skills is largely tied to the humanities. “When a recent survey asked executives what potential employees should study, a large majority pointed to the humanities so that students would develop stronger social skills and become better at reasoning and critical thinking” (Acton 42). A look at the cybersecurity bachelor degree programs for two universities suggests that there is at least some focus on the humanities:

George Mason University Cyber Security Engineering, BS - Credits



ECPI University Cyber and Information Security Technology, BS - Credits



However, studies find that “Many graduates emerge from cybersecurity education programs without these soft skills ... Problem-solving forms the very foundation of effective cybersecurity work, and many graduates face significant obstacles troubleshooting real-world systems” (Crumpler 5). An alarming 68% of organizations noticed a skills gap in soft skills among recent graduates, making it the most agreed upon skills gap, even over all technical skills (State of Cybersecurity 21). Unsurprisingly, critical thinking was highlighted as the number two most important missing soft skill, with a majority 54% agreeing (State of Cybersecurity 23).

These findings make it apparent that education systems are falling short in critical thinking development. Modifying curriculum to include a focus on critical thinking is a possible solution, though doing so would be a challenge. The curriculum must maintain a balance between technical and critical thinking focused courses, and as mentioned during a personal interview, “It is important to understand that modifying educational content at the university level requires accreditation. In order to maintain a high set of standards, learning content must

undergo a rigorous review process” (Weithers). With educational systems largely out of the hands of businesses, closing the critical thinking gap in the workforce presents a complex and challenging problem.

Does AI Replace the Need for Critical Thinking?

The need for critical thinking is overwhelmingly supported by the security community, but implementing it is a subject of debate. This is largely due to the costs associated with developing workforce critical thinking skills. “Addressing the shortcomings of educational systems often falls to employers, who must invest in extensive on-the-job training to bring these individuals up to speed” (Weithers). With the prevalence of artificial intelligence continuing to grow, it is arguable that its existence negates the need for security professionals to be trained in critical thinking at all. It is true that “AI can handle tasks more accurately and faster than a human does, thereby freeing up valuable time” and that “Company funds can alternatively be spent on maintaining AI systems rather than on hiring and training multiple employees to handle those (cybersecurity) tasks” (New Jersey State).

Further, malware analysis, a critical thinking focused task as previously discussed, can easily be automated using AI. In fact, “detecting advanced malware is one of the most successful uses of deep learning and AI technology” (Yaqub). This is just one of many examples of critical thinking oriented tasks that AI can automate, and as 62% of enterprises have either at least partially or fully implemented AI for cybersecurity (Yaqub), the question shifts from “how do we train critical thinking” to “why do we need critical thinking?”

Some argue that artificial intelligence will actually increase the demand for human cybersecurity professionals. “Despite concerns that AI might replace human expertise in this

field, it is becoming increasingly evident that as AI-based technologies mature, the demand for cybersecurity professionals will increase even further. Contrary to popular opinion, AI will be the primary factor increasing the demand for cybersecurity professionals” (“Key Cybersecurity Skills Gap Statistics”).

The more obvious aspect of AI, though, is that they “cannot generate new ideas or develop novel solutions on their own ... Human researchers can question and seek new knowledge by examining the world, while AI systems can only process preprogrammed information” (Randieri). It is true that the role of artificial intelligence mimics critical thinking by using pre-existing data to calculate an objectively good decision, but contemporary research suggests that “AI-based algorithms and systems should not be used exclusively for cybersecurity decision-making. Instead, to enable better decision-making processes, AI-based approaches should be firmly interwoven with human action” (Kaur 23). Thus, while artificial intelligence may help streamline a security professional’s workflow, critical thinking will remain central in an organization’s security posture.

Implementing Critical Thinking Best Practices

Rather than rely on institutions of higher learning, businesses may see benefit in implementing practices that foster critical thinking in the workplace. With the most common employer benefit being “pays employee certification fees” for the past two years (State of Cybersecurity 17), cybersecurity companies shouldn’t be too surprised that their focus on technical training has left critical thinking as one of their largest skill gaps. Fortunately, there has been some research into how businesses may begin to implement practices that work to combat the lack of critical thinking in the workplace.

Studies have found a “significant correlation between high cognitive diversity and high performance” (Reynolds), finding that “The three teams that completed the challenge in a good time all had diversity of both knowledge processes and perspective” and “The three that took longer or failed to complete all had less diversity.” Similarly, The Biden and Harris administration’s 2023 National Cyber and Workforce Education Strategy has identified “[strengthening] the cyber workforce through greater diversity and inclusion” (Office of the National Cyber Director 2) as one of its three core principles. It asserts that “To advance our collective prosperity, security, and well-being, we must draw on the full diversity of the American talent pool. Improvements in diversity, equity, inclusion, and accessibility in cybersecurity have tremendous potential to strengthen the cyber workforce, including gains in innovation, creative problem solving, improved decision making, and profitability” (Office of the National Cyber Director 5). Embracing cognitive diversity attacks common enemies of critical thinking, including confirmation bias, the tendency to favor information that confirms one’s existing beliefs, and groupthink, the desire for conformity (O’Sullivan). As such, businesses may see an increase in critical thinking by approaching their cyber workforce with cognitive diversity in mind.

In order to foster an environment of cognitive diversity to promote critical thinking, the global security community can look to leading companies like Google who have openly expressed their commitment to diversity. A 2020 blog reveals that Google seeks to effectively blend four personalities, citing that “healthy teams use their diversity to tackle new challenges” (Yorke). These four personalities are:

- Pioneers: curious, seek out new information

- Guardians: pragmatic, want to see evidence before making decisions
- Drivers: assertive, generate momentum
- Integrators: empathetic, rely on intuition to get groups to communicate better

Companies may also work to combat critical thinking shortages by implementing routine tabletop exercises, a form of cyber drill that aims to mimic real-world cyber threats to an organization. Tabletop exercises allow companies to gauge the ability of the security team to respond to incidents: “Effective tabletop exercises engage the audience by asking them to think critically, make difficult decisions, and rise to unforeseen challenges based on changing conditions and the actions they choose” (Pironti). Further, by adding stress events throughout the exercise, a company can stimulate critical thinking. “To be realistic, tabletop exercises should include stress events that are not accounted for in training or materials, but that need to be considered and addressed in real time during the test. Stress events should be challenging, difficult, confusing, and somewhat ambiguous to force the group being tested to question their current courses of action and consider new variables” (Pironti). Further research must be conducted to concretely establish correlation, but as critical thinking has been proven to be closely correlated with performance (Ejiogu 2), it would be beneficial for businesses to implement these practices.

Conclusions

The cybersecurity landscape is faced with a dual challenge: filling a multitude of vacancies and addressing a pervasive skills gap that extends beyond technical acuity. This paper has highlighted the crucial role of critical thinking in cybersecurity, underscoring its necessity

amidst the unpredictable nature of cyber threats. The evidence presented from various studies and expert opinions consistently reinforces the idea that without robust critical thinking skills, even the most technically proficient cybersecurity professionals might struggle to effectively adapt to dynamic security challenges. Therefore, while technical skills are indispensable, they must be complemented by strong critical thinking abilities, with the security community pivoting from an exclusive focus on certifications and positional requirements to an increased emphasis on critical thinking.

It is evident that educational institutions currently lack sufficient emphasis on developing the critical thinking skills required in the cybersecurity field. This deficiency not only hampers the ability of new graduates to perform effectively but also places an additional burden on employers to bridge this gap through extensive training programs.

Furthermore, the emergence of artificial intelligence in cybersecurity presents a nuanced challenge. While AI can automate and enhance certain tasks, it fundamentally lacks the ability to innovate or think abstractly in response to novel threats. Therefore, AI should be viewed as a tool that complements, rather than replaces, the critical thinking capabilities of human cybersecurity professionals.

To address these challenges, it is recommended that both educational systems and business practices evolve. Universities should integrate a balanced curriculum that promotes critical thinking alongside technical training, ideally supported by accreditation standards that recognize the importance of these skills. Concurrently, businesses should invest in creating environments that foster critical thinking, such as implementing cognitively diverse teams and conducting challenging tabletop exercises. These initiatives can provide cybersecurity

professionals with the cognitive tools needed to navigate complex and evolving threats more effectively.

As the cybersecurity landscape continues to evolve with increasing sophistication of threats, the importance of critical thinking remains paramount. Strengthening this skill is not merely an educational issue but a strategic imperative that will determine the resilience of our future cybersecurity workforce. By fostering an environment that encourages critical thinking, we can ensure a more secure and robust response to cyber threats, safeguarding our digital landscape for years to come.

Works Cited

- Acton, Peter. "The Capabilities Gained from Studying History Will Get You a Good Job, Studying STEM might Not." *Agora*, vol. 59, no. 1, 2024, pp. 41-44.
- Costanzo, John. *Bridging the Cybersecurity Talent Gap in Hampton Roads*. HRCyber, April 2018.
- Crumpler, William, and James A. Lewis. *The Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS), 2019, <http://www.jstor.org/stable/resrep22540>.
- Ejiogu, Kingsley C., et al. *Understanding the Relationship between Critical Thinking and Job Performance*. Pearson TalentLens, 2016, www.talentlens.com/content/dam/school/global/Global-Talentlens/uk/AboutUs/Whitepapers/Critical-Thinking-and-Job-Performance-white-paper_1.02.pdf.
- FBI Internet Crime Complaint Center (IC3). *2023 IC3 Annual Report*. Federal Bureau of Investigation, 2023, <https://www.ic3.gov/Home/AnnualReports>.
- ISC². *2023 ISC² Cybersecurity Workforce Study*. 2023, media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.
- Kaur, Ramanpreet, et al. 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions'. *Information Fusion*, vol. 97, 2023, p. 101804, <https://doi.org10.1016/j.inffus.2023.101804>.
- "Key Cybersecurity Skills Gap Statistics You Should Be Aware of." *Help Net*

Security, 2 Jan. 2024, www.helpnetsecurity.com/2024/01/02/cybersecurity-skills-gap-statistics/.

Morgan, Steve. "Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025."

Cybercrime Magazine. Cybersecurity Ventures, cybersecurityventures.com/jobs/.

New Jersey State, Legislature, Assembly. *Seeing AI to AI: Artificial*

Intelligence and Its Impact on Cybersecurity. New Jersey Cybersecurity and

Communications Integration Cell, 16 Jan. 2019, [www.cyber.nj.gov/](http://www.cyber.nj.gov/guidance-and-best-practices/artificial-intelligence/seeing-ai-to-ai-artificial-intelligence-and-its-impact-on-cybersecurity)

[guidance-and-best-practices/artificial-intelligence/](http://www.cyber.nj.gov/guidance-and-best-practices/artificial-intelligence/seeing-ai-to-ai-artificial-intelligence-and-its-impact-on-cybersecurity)

[seeing-ai-to-ai-artificial-intelligence-and-its-impact-on-cybersecurity](http://www.cyber.nj.gov/guidance-and-best-practices/artificial-intelligence/seeing-ai-to-ai-artificial-intelligence-and-its-impact-on-cybersecurity).

O'Sullivan, Michael. "Critical Thinking: An Essential Skill for Security

Professionals." *The Professional Security Officer Magazine*, 29 Dec. 2023,

[theprofessionalsecurityofficer.com/](http://theprofessionalsecurityofficer.com/critical-thinking-an-essential-skill-for-security-professionals/)

[critical-thinking-an-essential-skill-for-security-professionals/](http://theprofessionalsecurityofficer.com/critical-thinking-an-essential-skill-for-security-professionals/).

Pironti, John P. "Five Key Considerations for Developing Crisis Management and

Incident Response Tabletop Exercises." *At ISACA*, vol. 48, 29 Nov. 2023.

ISACA, [www.isaca.org/resources/news-and-trends/newsletters/atisaca/](http://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises)

[2023/volume-48/](http://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises)

[five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises](http://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises).

Ponemon Institute LLC. The Third Annual Study on the State of Endpoint Security

Risk. Ponemon Institute, Jan. 2020, [www.morphisec.com/hubfs/](http://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf)

[2020%20State%20of%20Endpoint%20Security%20Final.pdf](http://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf).

Office of the National Cyber Director. *National Cyber Workforce and Education Strategy*.

Executive Office of the President, 2023,

<https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf>

Ramezan, Christopher A. "Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field." *Journal of Information Systems Education*, vol. 34, no. 1, 2023, pp. 94-105.

Randieri, Cristian. "Can AI Replace Human Curiosity?" *Forbes Tech Council*, 22 Mar. 2023. *Forbes*, www.forbes.com/sites/forbestechcouncil/2023/03/22/can-ai-replace-human-curiosity/?sh=3f8984731991.

Reynolds, Alison, and David Lewis. *Teams Solve Problems Faster When They're More Cognitively Diverse*. Harvard Business Review, 30 Mar. 2017, hbr.org/2017/03/teams-solve-problems-faster-when-theyre-more-cognitively-diverse?referral=00060.

Schmidt, Lara, et al. *Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector?* RAND Corporation, 2015.

Sharif, Mohammed, et al. "A Literature Review of Financial Losses Statistics for Cyber Security and Future Trend." *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, 30 July 2022, pp. 138-56, <https://doi.org/10.30574/wjarr.2022.15.1.0573>.

State of Cybersecurity 2023. 2 Oct. 2023. *ISACA*, www.isaca.org/resources/reports/state-of-cybersecurity-2023.

Tripwire Guest Authors. "What Is the Most Important Skill Cyber Security Professionals Can Possess? The Experts Weigh In." *State of Security*, Tripwire, 16 Sept. 2018, www.tripwire.com/state-of-security/important-skills-cyber-security-professionals.

Weithers, Patrick. Personal Interview. 15 Feb 2024.

Yaqub, Mohammad. *AI in Cybersecurity: Statistics, Example and Trends in 2023*. 16

May 2023. *BusinessDIT*, www.businessdit.com/ai-in-cybersecurity/.

Yorke, Zachary. "How to Harness the Power of Inclusivity on Remote Teams."

Life at Google, Google, 9 Sept. 2020, blog.google/inside-google/

life-at-google/how-harness-power-inclusivity-remote-teams/.