Strengths

Effective communication is an everyday essential in my role as a coach and teacher, where I must articulate instructions, feedback, and strategies clearly to engage my learning outcomes with students and players effectively. Developing strong communication skills also allows me to engage with parents and colleagues more effectively, ensuring that everyone is aligned towards our common goals and striving towards our high standards. Thus, being a transferable skillset in cyber security when working as a team to protect organizations and people.

Time Management: Balancing multiple roles, such as teaching physical education TK-4th Grade and coaching 3 soccer teams, as well as pursuing a career in CyberSecurity requires meticulous time management. By efficiently organizing my schedule and prioritizing tasks I ensure that each responsibility receives the attention it deserves, leading to better outcomes for my students and athletes.

Leadership and Team Building: Leadership in coaching and teaching involves not just guiding individuals but also fostering a sense of teamwork and sharing a goal which we achieve through hard work, perseverance, and the ability to work cohesively. Furthermore, this is a strength that I use in my everyday life as I go throughout my day coaching and teaching collective responsibility by keeping the standards high, giving back positive feedback, and praising those who reach the standards causing them to strive towards greatness more.

Values

One of the values I have and contribute to organizations results from my character and my values. My core values consist of being able to adapt, continuous learning and applying it every day, inclusivity and equal opportunities, and the ability to protect people and data. In my experience, I've learned that being flexible and responsive to changing situations is key to success. Whether it's adjusting due to unexpected weather, errors with computers and programming, dealing with hackers, adapting my schedule to meet the diverse needs of individuals, or quickly shifting strategies, I thrive off environments where I can pivot around and find a common ground solution.

An

1. **What most interests me about the field of cybersecurity?**

What excites me about the field of cybersecurity is a very complex question to answer. Growing up I wanted to be a firefighter, doctor, and soccer player, and as I graduated from college changing my passion to pursue my doctorate in Physical Therapy. I found myself seconds away from enrolling in USC's DPT program. But it just didn't feel right. It did not feel authentic and I am a firm believer in authenticity as it leads to being the best you. This action led me to do research and watch hours of YouTube videos of other individuals and their careers as well as reading and listening to audio books on how to be the best version of myself. This is where I ran into the YouTube channel 'ScammerPayback', where I watched hours and back-to-back videos

until I decided that it was something of interest. I continued to do my research and saw how the field combines problem-solving, continuous learning, and the ability to make a real impact for large groups not just 1-2 individuals. I'm particularly drawn to the challenge of staying ahead of cybercriminals, helping others keep their information safe, and constantly evolving to challenge myself. But what truly sparked this was getting hacked myself and losing money due to this situation as well as having to restart my whole bank account. It was a frustrating encounter and something I kept looking back at. Furthermore,I remind myself every day, "Am I getting challenged enough while also learning and getting better"? That is why, why I decided this field would be great for me while also engaging in everyday battles that will motivate me.

2. **Who is the audience for my professional statement?**

Everyone and anyone who is interested in my career path and story but more specifically cybersecurity recruiters, specific organizations, and government employers.

3. **In what ways can my strengths values and interest in cybersecurity support the security goals of various organizations?**

Adaptability: My ability to adapt quickly to new situations is crucial in cybersecurity, where threats evolve rapidly. My strength enables me to stay ahead of emerging risks, quickly learn and implement new technologies, and respond effectively to incidents. Organizations benefit from this flexibility, as it ensures that their security measures remain robust and up-to-date.

Strong Communication Skills: Effective communication is vital in cybersecurity for educating employees, collaborating with teams, and reporting to stakeholders. My ability to convey complex security concepts clearly and understandably helps foster a security-conscious culture within the organization. This leads to better adherence to security protocols and reduces the likelihood of human error, which is often a significant vulnerability.

Commitment to Continuous Learning: Cybersecurity is a field that requires ongoing education due to its constantly changing landscape. As someone who works in education, my dedication to continuous learning ensures that I stay informed about the latest threats, tools, and best practices. This proactive approach allows organizations to implement cutting-edge security measures, reducing the risk of breaches and ensuring compliance with industry standards.

Interest in Protecting People and Data: My strong motivation to protect individuals and data aligns directly with the core mission of cybersecurity. Organizations rely on professionals who are not only skilled but also deeply committed to safeguarding their assets and customer information. Your passion for this protection drives you to be vigilant and thorough, ensuring that all security measures are designed and executed with the utmost care. 100% Bought in.

Promoting Inclusivity and Equity: Cybersecurity is not just about technology; it's also about ensuring that security practices are fair and accessible to everyone. My value of inclusivity can help organizations design and implement security policies that consider diverse user needs and promote equitable access to resources and information. This approach enhances the overall

effectiveness of security programs and fosters trust within the organization and among its stakeholders.