

How I Would Introduce Myself Professionally

Mikael Sykes

Department of Cybersecurity, Old Dominion University

IDS 493 Electronic Portfolio Project

Professor Carin Andrews,

March 28, 2026

How I Would Introduce Myself Professionally

My name is Mikael Sykes. I am a Cybersecurity major with a focus on network security, ethical hacking, and system protection, and I am pursuing a bachelor's degree in Cybersecurity. During my studies, I have found myself becoming interested in learning about how systems are attacked and, more importantly, how they can be defended before the vulnerability is used to attack them. The two that interest me especially are ethical hacking and penetration testing because I am able to lead an ethical game as an attacker in an effort to protect organizations and their online properties.

What I am drawn to in cybersecurity is the aspects of problem-solving, technical analysis, and real-world impact. The world is rapidly evolving technologically, and with this evolution, professionally qualified people are increasing in number and are capable of detecting and preventing cyber threats. I also prefer to work with complex systems, identify defects, correct them, and improve their security. My desired career is one where I will be actively involved in making sure that sensitive information is not lost and individuals are able to trust the digital systems.

I also have a career plan for the next phase of my career, as I am nearing the end of my bachelor's degree in May 2026. I shall also pursue higher-level courses on ethical hacking, and by the time I am through, I shall be pursuing a master's level. Cybersecurity is not only a profession to me but also an area that involves lifelong learning and is adaptive, and that is what I am committed to.

Important Life Milestones.

The courses that I am pursuing as part of my academic program have been of significant interest to me on the topic of cybersecurity, and have aided me in settling on a career path. One of the most powerful courses was Intro to Cyber Security and Cyber Security Fundamentals. The classes provided me with the basics of threats, vulnerabilities,

and risk management. They taught me that cyberattacks can occur and that effective security controls are required. This is the knowledge that I acquired, and this sparked my curiosity and made me explore more in the field.

The other experience is one obtained in courses like Network and Security, network systems security, and Linux Systems to Cyber Security. Those classes provided them with the real-life experience of actual tools and settings. The experiences I had with Linux systems and the knowledge I have of how networks operate enabled me to develop a greater appreciation of the design of systems and their areas of weakness. Learning about network setups and how to secure networks has made me realize the importance of good system administration and how it helps deter attacks.

Another experience that assisted me is the Basic Cyber Program & Network (Python). Taking this course, I have come to understand that it is possible to use programming to solve a cybersecurity issue, whether it is automating a task, analyzing data, or discovering vulnerabilities. Python provided me with an alternative approach to problem-solving, and it helped to establish the importance of technical versatility in this field.

Besides, courses such as Cyber Law and Cybersecurity Ethics have made me more knowledgeable about the ethical and legal responsibilities of working in cybersecurity. The courses were centered on the notion that ethical hacking is not just a technical skill; it is a question of integrity, responsibility, and the perception of the law. This has been particularly important since I have been considering a future career in ethical hacking.

Among these courses, which I am currently studying, are Cyber Criminology Fundamentals, Cybersecurity Ethics, and Entrepreneurship in Cybersecurity, which will help me further develop my understanding of the implications of cybercrime for society and the application of cybersecurity in business. These experiences are also enabling me to gain a wider view of the relationship between technical abilities and real-life challenges.

What I Learned Along the Way

All these educational experiences have enabled me to gain some of the valuable skills and know-how that have played a significant role in my professional self. Analysis is one of the most important skills I have gained. Cybersecurity requires the ability to investigate systems, identify tendencies, and identify possible threats. The way that my coursework has taught me to deal with problems has taught me to think critically regarding how vulnerabilities may be exploited and avoided.

I have also acquired good technical skills, particularly networking skills and system administration, as well as working on Linux environments. These are valuable skills that teach you how systems work and how to protect them. Passing a course in Python-based programming has also enhanced my skills in process automation and problem-solving, which are useful in current cybersecurity practice.

Another valuable lesson that I have learned is persistence. The majority of cybersecurity problems are complex and require time, patience, and trial and error to overcome. I have been in laboratories and also when troubleshooting my systems, and I need to stay focused and continue working until I can find a solution. This conclusion has made me trust my ability to cope with complex technical problems.

Furthermore, I have acquired additional knowledge of the ethical accountability behind the cybersecurity problem. I have learned about cyber law and ethics, and I have realized that high ethical standards should determine the technical skills. This is more when it comes to ethical hacking, whereby professionals are entrusted to discover the vulnerabilities without necessarily inflicting harm.

Finally, I have realized that technology is not all, and some people are engaged in cybersecurity. Human behavior, decision-making, and awareness are involved in system

security. This has made me understand how communication and education can be applied to prevent cyber threats.

Where I Am Headed

In the future, I will be an ethical hacker/penetration tester. The domains of my special interest are positions where one has to identify vulnerabilities of a system, test security systems, and help organizations to establish their overall security posture. These topics align with my interest in problem-solving and my willingness to be a proactive individual in cybersecurity.

After earning my bachelor's degree in May 2026, I will continue my education with a master's degree in cybersecurity or another related field. In addition, I intend to obtain industry-received certification on ethical hacking to further my knowledge and career opportunities. This area is also a prerequisite for constant learning, and I would commit myself to staying abreast of new technologies and threats.

New opportunities in cybersecurity entrepreneurship would also be a topic I would like to discuss. Courses like Entrepreneurship in Cyber Security have presented me with the concept of coming up with solutions to practical security problems. This could be a consideration when I create my own cybersecurity services or when I make contributions to new security solutions in the future.

Long-term, I would like to operate in an environment where I could apply my abilities to protect organizations, carry out significant projects, and grow as a cybersecurity expert. I am motivated by the difficulty of managing cyber threats and the opportunity to do good in an ever-more digital world.