Building Security Warrior 2.0

by Kim L. Jones CISM, CISSP, M.Sc.

I've had the privilege through most of my career to have known some very smart and thought-leading people. These people regularly push me to the edge of my comfort zone, and make me think about things differently.

Recently, one of these individuals asked me to explain why I had entered academia after so many years in industry, and what I was hoping to accomplish. After some thought, I said to her, "I'm hoping to create a program which produces the next generation of security warriors." My friend quickly pointed out that a) there are many Cybersecurity programs which already claim to be doing this; and b) the term "warrior" associated with Cybersecurity professionals has become "somewhat overused."

I spent some time explaining my position, describing why the foci of my program might be different from others and why I felt the term "warrior" was absolutely appropriate. In this first of a series of white papers, I'd like to share these thoughts with you.

This first white paper could best be described as my "Security Warrior 2.0 Manifesto." Here goes…

1. **Defense Alone Is Not Enough**. The former commander of Cybercom, General Keith Alexander, coined the phrase "Cyber Network Operations (CNO)" as a better definition of what we commonly refer to as Cyberwarfare. CNO is broken up into 3 parts: Cyber Network Defense (CND), Cyber Network Attack (CNA), and Cyber Network Exploitation (CNE). While CND is absolutely critical, most cyber professionals look at this as a zero-sum game. We layer our defenses; buy the neatest, latest tools; and hope they are sufficient to defeat (or at least discourage) potential attackers. While I do not advocate organizations exercising CNA, developing the skills and mindset necessary for CNA and CNE within organizations allows you to better protect your critical assets. "Thinking like the bad guy" needs to become more than a catch phrase; it should be

something that is taught, nurtured, and/or fostered within our security organizations. Only in this fashion can we truly protect our assets against the types of attacks and challenges that we are likely to face in the real world.

2. **Security Is an Interdisciplinary Problem**. In addition to the well-rounded aspects of any accredited degree program, there are five families of competencies of which any good security professional must have some working knowledge:

- Network Fundamentals and how to secure them
- Application Fundamentals and how to secure them (including how applications interact with data
- Governance and Privacy Fundamentals
- Risk Management
- Communication and Leadership Skills (speaking, writing, organizational psychology, ethics, time management, etc.)

By their very nature, these competencies cross lines between technical and non-technical areas. A person with training in just the technical competencies will be limited in their ability to appropriately articulate the risks of a problem, will fail to adequately understand the role of governance structures in solving that problem, and will lack the ability to communicate the problem or solution effectively. A person with training in just the non-technical competencies will lack the technical expertise to understand how to implement an effective solution, and may create governance structures that aren't supported by the technical footprint of the organization. We must create security professionals with the foundational knowledge, skills, and abilities in all 5 competency families.

3. **We Need to Bring Back Critical Thinking**. In the last security organization I ran, I had a mantra that went like this: "Making lemonade out of lemons is easy. The job of any security professional is to make lemonade out of two apples, a grapefruit, and a kumquat, and make it look easy." Finding creative solutions to problems is the security professional's job. Finding new and innovative ways to exploit the network so that we can defend against these exploits is also a security professional's job.

Security professionals need to be aware of the box, but need to be comfortable looking beyond the box for both challenges and solutions. This requires truly multi-dimensional thinkers who aren't content with just the most obvious answer and have the ability to look beyond what the logs show at face value. It also requires folks who understand that the answer to the problem will most likely not be found via a search engine. Unfortunately, many graduates of today's academic institutions are leaving without an appreciation for/passion for/grounding in these qualities.

4. **You Do Not Have the Option to Not Communicate**. One of the terms I used to affectionately describe some of my more technical resources is "pizza boys." These are the folks that I could lock

in a room, shove pizza under the door, and ask them to solve any problem in the company…but I could not ask them to chat with another non-technical person in the company. In today's world, that is not necessarily good enough.

As security professionals, we have long sought for the elevation of security to the attention of the C-suite and the Board of Directors. Congratulations; we have gotten our wish. It is now incumbent upon us to better communicate the problems, issues, and challenges faced within the realm of security. While I do not expect a 22-year-old InfoSec analyst to be comfortable speaking directly to the Board president, I do expect said analyst to understand the fundamentals of communication, how people process information, how to write in complete sentences, how to formulate an argument, how to begin to translate technical jargon into English, and how to carry on a conversation with a non-technical peer. In small shops and fluid environments (and let's face it: all of our shops are short staffed, and all of our environments are fluid), you will not always have the option to place a senior security body in front of someone for an answer. Their first contact may be the most junior member of your team. While that person will most likely not give them as cogent an answer as the CISO, their business colleagues should still walk away feeling like a reasonable communications effort has been made by a very competent security professional.

5. **Reality Matters**. One of my hobbies is that I teach and train in martial arts. At my first dojo, I remember the day when a very young and physically fit man came in and arrogantly declared, despite having never taken a single martial arts class, that he felt he was capable of taking on "the best the dojo could offer." My sensei smiled, and asked me — a 40-year-old 250+ pound man with a pot belly and bad knees — to go onto the mat with him. After 2 minutes, this fit and agile young man was breathing heavily. After 3 minutes, he had stopped being able to deflect my punches and kicks. After 4 minutes, he conceded the round. My sensei gently walked up to the young man and said to him, "You may be fit, but the only way to train to spar is to *spar*."

In similar fashion, students should be encouraged (if not mandated) to go out into the real world and work on real-world problems in real organizations as part of their course of study. While I applaud and wholly support the need for our higher institutions to engage in research-driven innovation efforts, these should not be considered an adequate substitute for opportunities to obtain real-world experience. (Note to the CISOs reading this: this means YOU need to be willing to take on and mentor interns within your organization, and give them experiences that go beyond just fetching coffee and making copies.)

6. **Information Assurance (IA) and Cybersecurity are Neither Synonymous nor Mutually Exclusive**. Most of us remember when the term Information Assurance came into vogue. Properly defined, IA refers to the steps involved in protecting information systems. It emphasizes the programmatic and process elements of security which are designed to ensure the confidentiality, availability, and integrity of assets. Seemingly overnight, colleges and universities were placing additional emphasis on governance programs, risk management, and the management portions of security. In doing so, we created a generation of assurance professionals who understood the

programmatic elements, at the potential expense of the technical skills and abilities to effectively combat threats. Part of that result, in this writer's opinion, has been the increased volume and severity of data exposures, combined with the erroneous labeling of such attacks as "sophisticated."

In recent years, in response to this paradigm, the pendulum has swung towards an almost fanatical and myopic focus on cyber technical skills. Just as we saw the creation of IA programs in the early 2000s, we're now seeing a spate of Cybersecurity programs focusing on the tactical and technical skills to combat threats. Programmatics and governance have become something of an afterthought; in the race to create more technical assets, we are producing a set of cyber professionals without an appropriate grounding in programmatic security skills.

The reality of the situation is that IA and Cybersecurity are both necessary to win the fight. Properly defined, Cybersecurity is a subset of IA. Any good IA program needs talented, capable technologists in order to drive a successful defense against potential threats. Instead of creating an either/or paradigm, security warriors should advocate and promote the existence of both technical and programmatic security elements. While initiatives and approaches such as DevSecOps and Rugged Software may allow for a decreased emphasis on the IA function, IA is an expression of security governance and governance plays an important role in any organization.

* * * * *

Security Warrior 2.0 is an individual who:

- is highly technically skilled;
- has the ability to think critically;
- understands the tenets of governance, privacy, and risk;
- can communicate their ideas in a cogent fashion;
- has had some real world experience solving real world problems in a real-world environment; and
- has the potential and the foundational skills to thrive in any role within the security organization

I firmly believe that creating such an individual is not beyond the reach of our very talented and very dedicated global security community.

My two cents…

About the Author

Kim L. Jones is a 30-year intelligence, security, and risk management professional with expertise in information security strategy; governance & compliance; security operations; and risk management. A sought-after speaker and industry thought leader, Professor Jones is a former Chief Security Officer who has built, operated, and/or managed information security programs within the financial services, defense, healthcare, manufacturing, and business outsourcing industries.

Jones holds a Bachelors Degree in computer science from the United States Military Academy at West Point, and a Masters Degree in Information Assurance from Norwich University. He also holds the CISM and CISSP certifications.

Professor Jones may be reached at kimjones.cism@asu.edu. You may also read his postings at www.security2cents.com.