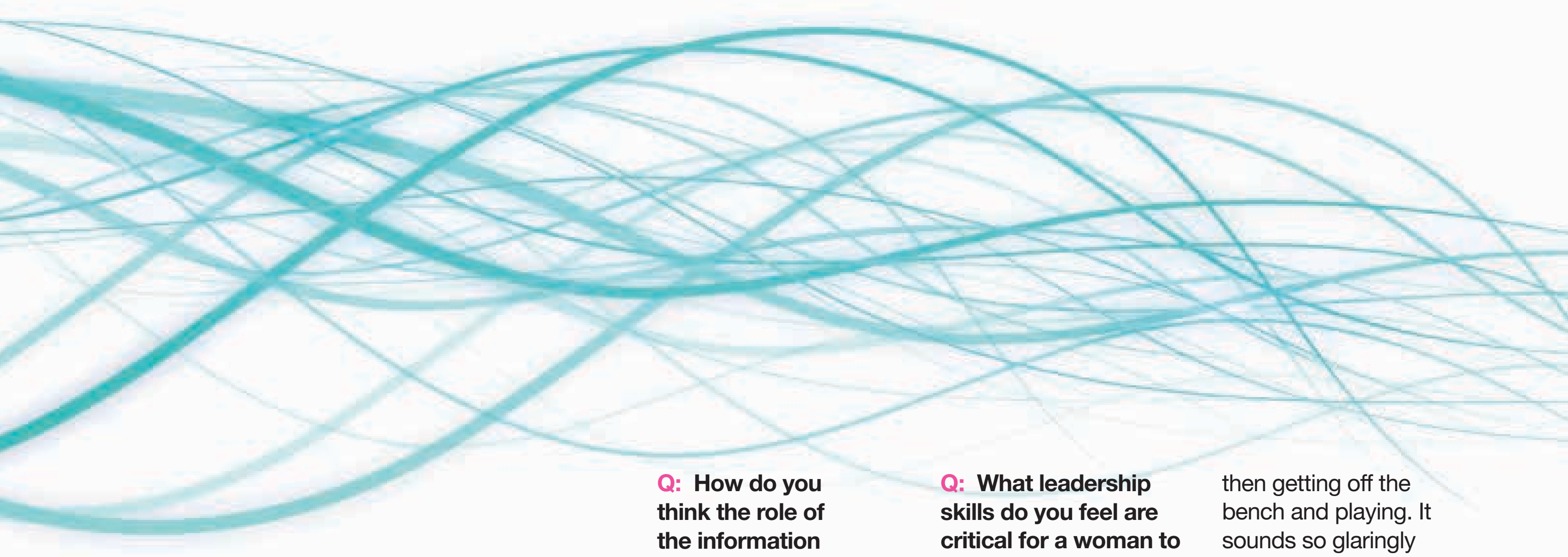

Shan Senanayake, CISA, CRISC, CISSP
Is promoting smart community involvement in cybersecurity and encouraging everyone within earshot to get trained in cybersecurity the same way you encourage people to take self-defense classes. Originally from Singapore, she has worked as an IT consultant and trainer in Singapore, Silicon Valley, New York, New Jersey and now Bermuda—a tiny, incredibly beautiful island in the middle of the Atlantic Ocean.

Q: How do you think the role of the information security professional is changing or has changed?

A: It is a more nuanced job nowadays, and the scope is certainly much broader than it was a decade or two ago. Information security is also now driving major aspects of organizational strategy instead of merely aligning with the business needs or outright taking its cue from it.

The information security professional has evolved from a role that was purely about compliance and managing technical controls behind the scenes to one that must understand corporate strategy and have the capability to sit in the boardroom and advocate strategic and behavioral change.

We security wonks used to have to strategize about getting buy-in from the executive level to implement security initiatives, but, nowadays, the folks in the boardrooms are the ones who are asking about the security posture, so we are pushing on an open door.

Q: What leadership skills do you feel are critical for a woman to be successful in the field of information security?

A: I would say self-determination is key—and it might be something above and beyond what male peers have to sustain. You must have resilience to opposition and the ability to forge a path where none exists. Maybe no other woman has done your job before you, so you do what any explorer does when there is no well-trodden path. You make your own.

In many other respects, women require the same leadership skills that a man in the same position would—the assertiveness, ingenuity and empathy that make you a universally valuable and effective operator. A blanket statement about desirable leadership qualities in all women is considerably less useful than saying, “Be valuable where you are and where you want to go.”

Q: What is the best way for someone to develop those skills?

A: By figuring out which skills are required to excel, and then getting off the bench and playing. It sounds so glaringly obvious, but the two major requirements to developing any skill are deciding what to learn and then practicing. If you are lucky, you have guidance; a mentor to chivvy you along. If not, do not be afraid of trial and error. Learning to fail is a useful skill in itself. You can optimize the likelihood of success by learning what does not work.

Q: How have the certifications you have attained advanced or enhanced your career?

A: I work in the IT and security sphere, so the bulk of my certifications tend to be related to technology: networking equipment, operating systems, virtualization platforms. You need to know how to make the infrastructure work; that is the priority for IT. However, there is enormous value in having vendor-neutral security qualifications, such as the Certified Information Systems Auditor® (CISA®) and Certified in Risk and Information Systems Control® (CRISC®). It means that the people who build and maintain the infrastructure know that it must align with

the network

She Leads IT

security methodologies. Not enough IT professionals understand how to do this and it is a huge professional advantage to be able to do so.

Q: What do you think are the most effective ways to address the lack of women in the information security workspace?

A: Ever hear the saying "No one becomes an astronaut by mistake"? The same is true for many terrestrial aspirations such as information security. There needs to be a road map and the impetus to follow it. I think ISACA's CSX initiative for students—to lower the barriers to entry to a career in information security—is exactly what is needed. A career in information security must be a visible, viable option.

Regardless of gender, we are looking at an industrywide supply chain issue. We do not have nearly enough information security professionals, and this is not something that can be corrected overnight. We need a groundswell, a revolution of participation, and it needs to begin in early education and be sustained all the way through college.

I think lowering the barriers to entry and raising the visibility of women in the profession would go a long way. Women in information security need to be normalized and there needs to be guidance. Many of the younger women whom I have met in the information security community have been mentored or have followed a structured educational path to get here. Very few became Infonauts by mistake.

Q: How did you arrive at a career in information security?

A: I started out as a techie in Silicon Valley during the boom years, when there were not a whole lot of rules about how you had to use technology in the enterprise. So you figure out how to do things when there is no guidance. You hack the infrastructure together and roll your own kernels, because vendor interoperability is still a ways off. In retrospect, it was a hugely useful way to start out in the industry, because you learn very early on to be curious and adaptable, or you perish. You also learn to appreciate the value of ordered chaos, which all networks are, in essence.

Q: What has been your biggest workplace or career challenge and how did you face it?

A: When I was an itinerant consultant, I was having so much fun with my great customers, interesting projects and an endless parade of new technology to play with that I did not want to admit to myself that I had hit a glass ceiling at the consulting firm. This had a hugely detrimental effect on my career progression and it was an obstacle that could not be removed, countered or mitigated.

In hindsight, what makes this incident stand out for me is that I expended so much effort trying to change the culture that I had become inured to the extra effort. As soon as I moved to a more progressive environment, I was able to accomplish much more. It is a very important realization to have—that the environment should be actively helping you achieve your goals. That experience forever impressed upon me the importance of culture change with the end goal of a achieving a meritocracy.

www.sheleadsit.org

1 What is the biggest security challenge that will be faced in 2017? How should it be addressed?

Resisting the push toward "exceptional access"—mandated back doors for law enforcement (think US Federal Bureau of Investigation [FBI] vs. San Bernadino iPhone).

2 What are your three goals for 2017?

- Run a 10k
- Paint outdoors
- Read 52 books (I try this every year and have never made it to 52.)

3 What is on your desk right now?

- Stickerless Rubik's Cubes in various stages of solved
- A stack of purring network switches
- A bowl of coral bits that washed up on the beach, bleached white from the sun

4 What is your number-one piece of advice for other information security professionals?

Do not be deterred by an unfamiliar or unwelcoming culture. You are an ambassador for whatever you are representing or advocating, and you have to be able to walk into a room full of strangers and evangelize information security.

5 What is your favorite benefit of your ISACA membership?

The worldwide ISACA community. I love getting to meet other IT security and audit professionals and talking to them about what they do.

6 What do you do when you are not at work?

Take advantage of all the wonderful things and technologies to which I have access. My two best friends are adventurers, always chivvying me to try something new. It is oddly relaxing.

Connecting Women Leaders in Technology

ENGAGE. EMPOWER. ELEVATE.

ISACA