Justine Bone
Is an information technology and security executive with a technical background in software security, risk management, information security governance and identity management. She has spent more than 15 years working in the private sector for financial, news and information security companies, plus several years serving the intelligence community. Over the past few years, she has been instrumental in evolving information security governance and strategy within the private sector. She has led MedSec as chief executive officer (CEO), served as the global chief information security officer at Dow Jones and acted as the global head of risk management at Bloomberg L.P. She was also CEO of boutique security research firm Immunity Inc., and founded an independent private intelligence service serving select US federal agencies.

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

A: We are really seeing diversification when it comes to the role of a cyber security professional. From the security operations center (SOC) to the engineering floor, from the dark web to the financial markets, these days we need folks who are not just fluent in cyber, but who have additional skills, capabilities or certifications.

I have a pet peeve: references to "soft skills." But I think we all recognize the need to go beyond purely technical capabilities. A colleague of mine recently said, "It's not soft skills, it's extrapolation in a higher form." I could not have said it better.

Additionally, most of us are happy to see cyber security getting the attention it needs from the boardroom on down. Again, communication skills are essential here. The job of the chief information security officer (CISO) is not just to present information, but also to persuade other decision makers about the best course of action.

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

A: Adaptability and a desire to continue learning are key. We need to be able to recognize shifts in policy, culture and business, and then understand the emerging technologies that might support those shifts. But that is a skill critical for any leader in cyber security. For women—I'll be honest—it is still pretty rough out there. As minorities, we are under heightened scrutiny and often need to address preconceptions by exceeding the standards applied to others. If you are pushing new ideas, this gets especially challenging because you are often doing so alone. So, being comfortable alone, being able to trust one's instinct and remaining confident in the face of adversity are some of the skills I rely on.

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

A: With regard to confidence, it starts by understanding the problem. I have yet to meet an over-confident women in technology, so let's make a safe assumption that there is or will be a problem related to lack of confidence for most of us. *The Confidence Code*, by Katty Kay and Claire Shipman, is a book that helped me understand why this can be such a struggle. It discusses how some kids (typically boys) are encouraged to take risks, as opposed to other kids (typically girls) who are rewarded for following the rules. This serves girls well as young children in school systems, until a certain point. But, eventually, the risk takers, who have been taught that it is okay to fail, go out into the world taking

risks with confidence. Understanding this has helped me relieve stress and make tough decisions.

Q: What advice do you have for information security professionals as they plan their career paths and look at the future of information security?

A: Think about a future where cyber security is a more generalized concept. As an expert, you might pick a technical path such as vulnerability researcher, forensic investigator or engineer, but also, you could be a lawyer specializing in cyber security, a policy expert or an educator. At some point, most folks need to make a decision about how technical they want to be—and I do believe that for most people, that is a choice. I believe anyone can understand the technology just as anyone can understand math. It is a function of communication—good teaching—and the way the information is presented to successfully learn the subject.

Q: What do you think are the most effective ways to address the cyber security skills gap and, especially, the lack of women in the cyber security workspace?

A: I would really like to focus on diversity as an opportunity as opposed to focusing on women (and the lack thereof) as a problem. We have real numbers now around increased company and economic performance with increased diversity, and I would like to see more research around that.

On a more personal front, I believe I can be most effective in leading by example. I feel a responsibility to work hard and fight the tough battles to make this a more accessible career for others who may not have that same appetite for challenge! We need those people, too—we do not all have to be pioneers out there breaking new ground.

Q: You took an unconventional road to the career field you have now, having started out as a dancer with the Royal New Zealand Ballet company. How did you arrive at a career in information security?

A: I do not really arrive somewhere, as much as plan my destination in advance! I had always been interested in computers and loved math. I also have a few traits that have driven me along the way, such as unrelenting ambition and the self-discipline to see plans through. I come from a family of planners. We plan everything to such an extent that we arguably live in the future. So, I always knew that after ballet I would try something more scientific as a disruptive and ambitious change.

I like to always be learning. I also like to change my environment frequently via travel, which is how I ended up living on the other side of the world from my family, and why we are always planning our next family rendezvous.

1 What is the biggest security challenge that will be faced in 2018?

Holding technology vendors and manufacturers accountable for low-quality product.

2 What are your three goals for 2018?

Help hospitals, travel more and improve at managing stress.

3 What are your favorite blogs?

Twitter and *The Wall Street Journal*.

4 What is on your desk right now?

My headphones, two laptops, my phone and dumbbells. I try to work out quietly when I am on long conference calls!

5 Who are you following on Twitter?

I have started following investors and others in the financial sector. We have a lot to learn from that crowd.

6 What is your number-one piece of advice for other information security professionals, especially women?

Being a minority is an opportunity. Yes, we often have to over-deliver to achieve similar outcomes to others, but as a result, we know our material inside out. In addition, many of us can rely on a multitude of skills—including communications skills—that others may not have.

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

Typically, I am either working or spending time with my kids, so I try to blend in things I enjoy with both. I love experiencing new cultures and places and, luckily, get to blend that with my work. When with the kids, music and the outdoors are high on the priority list. I am also beginning to work on a book. I have not done enough yet to determine whether or not that qualifies as work!