Building Tomorrow's Leaders Today

Kevin Murphy, CISM, CRISC, CEH, CIPM, CISSP, Dip PSLM, ISO 27001, LLB
Is an internationally award-winning cybersecurity professional and current president of the ISACA Scotland Chapter. His previous cybersecurity experience includes eight years as a police officer where he was awarded a chief constable's commendation and four years as part of KPMG's award-winning Cyber Security Team. Murphy now works for a global bank as a cybersecurity, privacy, risk and innovation specialist. He has authored two books on training and development, with a third, *Cybersecurity: Law and Practice*, due to be released in 2018. He is a noted speaker on the international security circuit and a regular contributor to leading cybersecurity, risk and privacy publications.

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

A: The breadth has changed. To be effective cybersecurity professionals, we must see ourselves as partners in the business, rather than "consultants" who are one step removed and take no responsibility. We can achieve this by always placing the voice of the customer central to everything we do, whether it be opening up our enterprise to share information with authorized third parties or designing a new web application interface—we must always reconcile security principles with an enhanced customer experience.

We cybersecurity professionals must acknowledge we are part of a new paradigm. Change can no longer be viewed as a threat, but an opportunity for growth. We can no longer operate and secure in isolation, but must act as part of a far wider technology ecosystem.

Q: What leadership skills do you feel are critical to be successful in the field of cybersecurity?

A: First, openness. To advise the business, you must understand the business and be prepared to be challenged. Listen to your key stakeholders; show a willingness to understand their concerns and risk scenarios. Find that common ground where you can work together and form a common goal.

Second, integrity. The concept of the modern organization is more fluid than ever. The data life cycle is infinitely more diverse and increasingly fragmented. This brings business opportunity, but also challenges in how to operate securely. As such, there can be great pressure to circumvent security to aid business growth. The cybersecurity professional must guard against this trend and not be afraid to be the lone voice in the room. To add credibility and bring others onside, always keep your opinions factual, supported by evidence and focused on the customer journey tied to business goals.

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

A: Increasingly, it is a given that the cybersecurity professional has industry recognized qualifications. Thus, for an individual to distinguish themselves, they must excel in soft skills—listening, presenting, and, essentially, doing the basics brilliantly (e.g., well organized, considerate, and independently problem solving without escalating).

For the all-important soft skills, there is no better way to learn than to volunteer. My own volunteer experiences include speaking in front of 400 people at national events (yes, I was nervous, but it gets easier!) and organizing international conferences and even a pub quiz. Each involved meeting new people, using my initiative to solve problems on the spot and taking responsibility while gaining and practicing new skills.

Q: What advice do you have for information security professionals as they plan their career paths?

A: Use ISACA to identify a mentor. When I transitioned from the Police Service to cybersecurity in the private sector, I, unfortunately, took a few wrong turns which was frustrating. Upon joining ISACA, I immediately sought out a mentor (Rory Alsop, former ISACA Scotland Chapter president) who was instrumental in providing career advice, interview

skills and helping with exam preparation. Ultimately, Rory even convinced me to join the local chapter board, which explains where I am today, and it has been immensely rewarding.

Q: What do you think are the most effective ways to address the cybersecurity skills gap?

A: To address the skills gap, we need to engage young people at the earliest age. My chapter has done great work engaging young people at both school and the academic level. Moreover, in Scotland, cybersecurity qualifications are offered in high school, which I hope shall filter through to increasing professional ranks in the medium term. I hope this grass roots approach encourages a new generation of professionals from all backgrounds.

Moving into 2019, I intend my chapter to focus on encouraging individuals from lower socioeconomic backgrounds to transition into cybersecurity, for example, by speaking at adult learning centers and engaging people who have been displaced by the recession of traditional roles (e.g., industry and manufacturing). As we move to a service economy, I would love ISACA to champion an initiative to help make cybersecurity a second, third, fourth career for those most in need; the talent is definitely out there!

Q: You have a background in law enforcement. How did you arrive at a career in information security and how does that experience inform your current work?

A: I have often said a career in law enforcement is the best leadership course in the world. You see people at their best and also at their worst. The moment you pull on that uniform no one knows if you have one day's experience or 10 years. They just expect you to take command and solve the situation.

During my service, I had experience serving in the high-tech crime unit; from there my interest in technology and security blossomed and I went on to achieve the CISSP. Ready for a new challenge, I transitioned to the private sector.

My ability to use my initiative and solve problems independently has definitely been the most valuable attribute I have taken from the police into the private sector—a characteristic I encourage all my staff to develop.

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

A: Moving from the police to KPMG as a cybersecurity consultant. I was so full of self-doubt I remember telling my family if I lasted three months I had done well.

Looking back, I absolutely loved the challenge of a new culture and learning a host of new skills from report writing to business development. I had a fantastic boss at KPMG (a fellow ISACA member) who was incredibly supportive. My mentor also had professional services experience and was a great sounding board.

It is exhilarating to keep pushing yourself outside of your comfort zone—a path from which I have never turned away. I would be the first to admit, however, that any success I have had has always been supported by others along the way.

1 What is the biggest security challenge that will be faced in 2019? How should it be addressed?
Ethical application of new technology. Whether it be enhancing security through user behavior analytics, or using AI to enhance automatic customer decision making, we must ensure we always act fairly and transparently.

2 What are your three goals for 2019?
- Read more.
- Smile more.
- Have more fun at work!

3 What is your favorite blog?
- Bruce Schneier (*www.schneier.com*)
- The technology section of the American Bar Association (*https://www.americanbar.org/groups/science_technology.html*)

4 What is on your desk right now?
Extreme Ownership by Jocko Willink and Leif Babin

5 Who are you following on Twitter?
@IsacaScotland, of course!

6 How has social media impacted you professionally?
Great way to engage new members which, I am glad to say, has increased by 55 percent in just five years!

7 What is your number-one piece of advice for other information security professionals, especially women?
Join your local chapter and seek out a mentor whose journey you would like to replicate. Also keep an eye out for the latest #SheLeadsTech news.

8 What do you do when you are not at work?
I love reading, traveling, cooking, exercise and being outdoors.