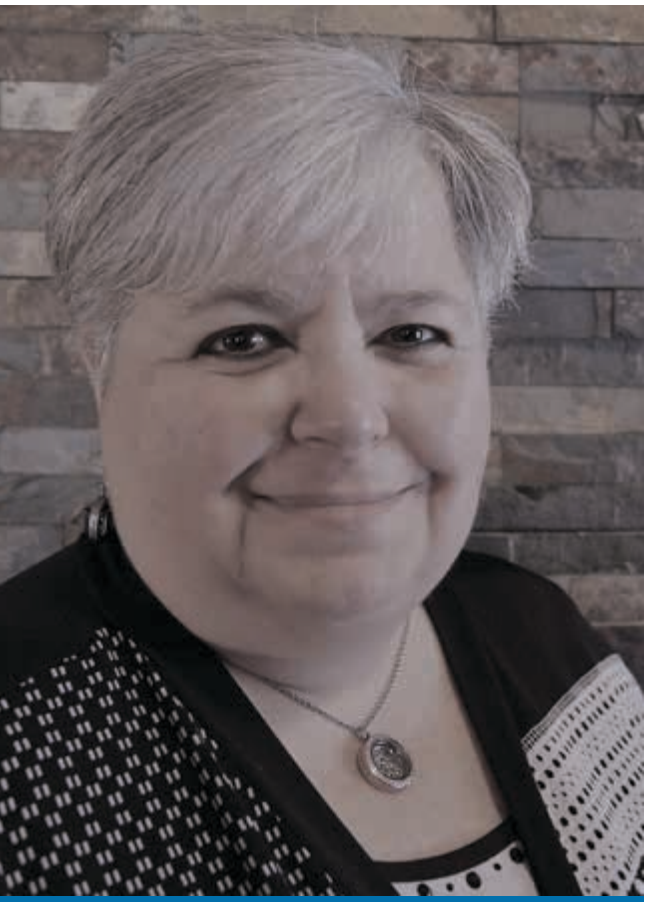
Building Tomorrow's Leaders, Today



Sandy Fadale, CRISC, CISM, CGEIT
Is a senior security consultant with Mariner Security Solutions. She has more than 25 years of in-depth IT experience in the field of enterprise computing with an emphasis on information security, which includes IT security, application development and business continuity. Prior to Mariner Security Solutions, Fadale was a senior manager at Bell Aliant, a manager with Ernst & Young LLP, and a manager with Visteon Corporation in its information security and risk advisory practices. She also served in the US military in telecommunications, utilizing various encryption techniques. She has been the president of the ISACA® Atlantic Provinces Chapter since 2008. Fadale teaches Certified in Risk and Information Systems Control™ (CRISC™), Certified Information Security Manager® (CISM®), and Certified in the Governance of Enterprise IT® (CGEIT®) certification review courses and is a subject matter expert who has assisted in the creation of the 2012, 2013 and 2014 editions of the ISACA *CRISC® Review Manual*.

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

A: It has long been said that employees are the biggest threat, but I do not believe that has ever been so true as it is now. I believe information risk management is one of the most important skills a security professional needs to possess today to provide value. From small start-ups to large organizations, information assets are leaving our organizations and the ability to understand where they are and how to secure them is extremely challenging.

Gone are the days we would issue edicts (back in the late 1980s and '90s). We are now advisors and we need to understand governance and compliance, privacy, metrics and data analytics, as well as business consulting skills.

Protecting information, no matter where it is located, requires a different way of thinking. Information security professionals who are used to concentrating on technology need to change their focus to business processes and data. Cloud computing and mobile devices are controlling this evolution; they are requiring that security professionals spend more time on governance and providing advice to organizations than on direct operational responsibilities for cloud and mobile environments.

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

A: I believe analytical skills are critical for information security professionals. Analytical skills refer to the ability to collect and analyze information, solve problems, and make decisions. These strengths can help increase and benefit an organization's productivity.

Employers look for employees who use clear, logical steps and excellent judgment to understand an issue from all angles before executing an action.

There are five skills that fall under analytical skills that I believe are important to master: communication, creativity, critical thinking, data analysis and research capabilities.

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

A: Having a mentor to teach you how to fine-tune analytical skills is really helpful. Do not feel as though you have ever mastered this area. Always continue to refine it.

But how do you go about selecting a mentor? Find someone to emulate, and study that person. Then ask him/her to be a mentor. Ensure that the person understands the area in which you want to grow and why you chose him/her. Continuously evaluate your growth and your mentored relationship. It may be awkward at first, but let the relationship develop organically. As the relationship grows and you are being challenged, do not run away.

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: This is not a cut-and-dried topic. It is extremely complex and usually depends on a combination of technical skills, nontechnical skills and personal interest. I do not believe that just anyone can be a technical security professional. One must understand networking, route switching, common hacking techniques plus many other areas. I have built my career on the people, process, governance and risk management side of the house. So, those starting a career must really understand which path they want to take: the super-cool "How do hackers think?" technical side or the governance, risk and compliance side.

How people gain knowledge is as individual as the individual. For example, you can go to university and specialize. Once university is completed and you are in a junior role, you can then pursue certification (and there are many of those). That said, however, just having a certification

and textbook knowledge does not automatically make an effective security professional. I worry that recruiters and human resources (HR) departments often rely too heavily on paper-based qualifications, given the pressing need to fill open positions.

Information security as a career choice is hugely rewarding. Regardless of the discipline chosen, security requires life-long learning and constant change. Security professionals never grow bored.

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: Part of the problem stems from the lack of information about careers in information security. This issue traces its roots all the way down to parents and school counselors not knowing about the full range of opportunities or, at best, reducing the field to looking only to the specialty of hacking. Often, parents and students are told that the only way to follow a security career path is to go through a traditional computer science program or a networking program, then switch into security. This may have been the reality 10 years ago, but it is no longer the case: An increasing number of schools are offering graduate and even undergraduate courses feeding directly into information security careers.

Organizations need to retain employees as the opportunities for switching jobs for more money are numerous in this field. Retention techniques include providing opportunities for continuing education and professional development and setting a clear path for development.

Information security professionals can work together to begin to make a difference in the cyber security talent shortage. Efforts can range from retraining existing employees, to recruiting high schoolers into specific educational pathways, to bringing together the government sector, private sector and academia to share amazing opportunities for employment and growth in the ever-expanding field of cyber security.

Q: You served in the US military. How did that experience shape your professional experience as a civilian?

A: When I was in the military in the late '70s, I got a taste of security as I set up encrypted communications channels using 16-bit encryption, and I knew this was the career for me. Security was not a "thing" after I got out of the military as a disabled veteran in 1980. However, in 1986, I went back to school and graduated with a computer science degree and then a security administrator position happened to come up in 1989 and I took it. The rest is history.

I think I was shaped by the military in my discipline and respect for people. I was raised that your word is everything and a handshake is binding, and the military reinforced that.

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

Working in a truly global organization several years ago, I was faced with understanding privacy laws, security laws and regulations around the globe. Security policies could not be written at a parent company and pushed out to its affiliates because countries' laws differed.

We had an incident in Italy that we needed to investigate. During the investigation, I received a call from our legal department asking what I was doing, so I told them. I was promptly advised that Italy has some of the strictest privacy laws in the world and I should not be able to see what I had seen. We ended up building a small data center there so information would remain in-country.

I had to update the policies to better reflect the laws around the world.

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

Continued cyberattacks from Russia and China

2 What are your three goals for 2018?

- Obtain my Certified Information Systems Auditor® (CISA®) certification
- Build Mariner Security Services (MSS) Training product line into a well-respected training offering in Atlantic Canada
- Help grow the MSS business

3 What is your favorite blog?

Krebs on Security @briankrebs

4 What is on your desk right now?

Coffee (decaffeinated), two monitors, wireless keyboard, wireless mouse and mouse pad, a light and my client notes notebook

5 Who are you following on Twitter?

Green Party Canada, Digital Forensics, Peter Morin, Paul Jauregui, TrendLabs, Think Progress, Kaseya, The IoT, Dark Reading, among others

6 How has social media impacted you professionally?

It allows me to have the latest trends at my fingertips.

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

Be confident in what you know. There is a fine line between assertion and aggression—do not cross it.

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

Spend time with my wife outdoors, camping, playing Pickleball and practicing yoga

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2kvEnvB