Gail Coury, CISA, CISM, CISSP
Has more than 20 years of experience in information security infrastructure systems and network management, security technical consulting, information systems auditing, and programming. She has worked in industries including software and hardware technology, airline reservation systems, insurance, banking and retail. She leads the risk management function for Oracle's Managed Cloud Services. This includes security strategy, security solutions, operational compliance, customer security services, audit compliance and delivery assurance. She is the former chief information security officer for PeopleSoft and former chief information security officer for J.D. Edwards.

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

A: Security leaders today are frequently advising senior management on information risk. Gone are the days when security people were only technicians who set the dials on who could access files or set firewall configuration to allow or deny traffic into the network. Then, security was seen as an IT issue. But today, businesses are more reliant than ever on technology to deliver products and services. Now, security is defending the enterprise from external cyberattack and enabling the business to continue functioning. With the frequency and magnitude of security breaches and the resulting business impact, the subject of information risk has moved to the board room.

This increased importance of information security led many enterprises to establish the role of the chief information security officer (CISO). Initially CISOs were very tactical and placed security goals above business goals. They became despised as they often objected to business goals as being insecure. They were called the ones who put the "no" in knowledge.

Today's CISOs need to broaden their technical skills to include business understanding. They need to communicate risk in business terms and help guide the balance of security risk and business strategy, knowing that there may be times when the company may accept more security risk in order to move the business forward.

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

A: First and foremost, you must be knowledgeable about information security, compliance and privacy. Your credibility as a leader depends on this.

You must also understand your business and your business strategy, and be organizationally aware—who are the leaders and what are their overall goals? With this information, you can use security as an enabler to help the business succeed and achieve its goals within an acceptable level of risk.

Also, successful security leaders are very good influencers—they are able to articulate risk in the language of the individual business and technology leaders. This skill helps get buy-in for the CISO's objectives.

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

A: We need to get in front of high school-age young women and communicate the opportunities that are available in this field as they contemplate their higher education options. Also, having a presence at large conferences through speaking opportunities or panels of women leaders can inspire women engineers or technical auditors to explore information security as an option.

Q: You took an unconventional road to the career field you have now. How did you arrive at a career in information security?

the network
She Leads IT

A: I graduated from college with a degree in computer science. I love problem solving and am a logical thinker, so it was the perfect fit for me. But being a developer sometimes required long or odd working hours. When I started a family, this became difficult. So I accepted a job as an IT auditor for a large local bank. I enjoyed using my problem-solving skills to look for weaknesses in systems.

After a number of years as an IT auditor, I was working for a large airline reservations systems company when the Internet began to be used to deliver services. The company was transforming from mainframes and hard-wired connections to distributed computing and, eventually, to Internet connections. The information security manager decided to retire and I was asked not only to step into that role, but also to remediate all the security issues I identified when I was their auditor.

A couple of years later, I was hired by J.D. Edwards to help form a security program. I was named the CISO in 2000. In 2003, J.D. Edwards was acquired by PeopleSoft and I was asked to stay on as the CISO for PeopleSoft, which was then acquired by Oracle in 2005.

Q: There is much discussion about the global cybersecurity skills gap. What do you think is the best way to encourage women to enter and remain in the field of cybersecurity?

A: This is such a fun and challenging profession—there are never two days that are the same. In some companies, it also provides opportunities to have flexible work schedules or work-from-home days that can help provide that work/life balance. However, keep in mind, it is a very high-stress career, and the time demands still exist, even with flexible work arrangements. It could still be challenging to start a family, but it may be easier now than it was when I started.

Cybersecurity is a profession that will continue to grow and expertise in this area will be highly sought after, which will drive up compensation.

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

A: It was a challenge to come into a new company as part of an acquisition and take on a leadership role. There was some skepticism among the ranks. I knew that I would need to establish my own credibility.

I asked a lot of questions and I listened to the answers. I shared what I was thinking and why with my team—then asked for their input. I made some hard and sometimes not-too-popular decisions, but I was able to explain my thinking with my management and my peers. And I made sure through influencing that my direct team was on board. I also made sure that stakeholders knew and understood the team's plans.

There were naysayers who said things had been tried before, but we did achieve success and the business benefited. And because of this success, the next undertaking was not quite as challenging—at least there were fewer naysayers.

www.sheleadsit.org

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

Cybercrime. The year-over-year growth is astronomical.

2 What is on your desk right now?

- A globe pinned with the places in the world I have traveled
- A basketball player's bobble head that has a picture of my son's face on the head
- An "art project" made of discarded/trash objects that my granddaughter made when she was in day care.
- A small plaque from United Airlines commemorating the million air miles that I have flown with them

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

Know your stuff, stay current with changing technologies, and understand your business and where it is headed.

4 What is your favorite benefit of your ISACA membership?

Being part of the Connecting Women Leaders in Technology program. I also appreciate the *ISACA® Journal* for keeping up to date on security concerns.

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

I am a huge Denver Broncos fan, so during football season, I follow the team and all their games. Otherwise, I spend my time with my family: my husband who also happens to be a CISO (you can imagine our dinner conversations), my six children and their spouses, and my eight, soon to be nine grandchildren.

Connecting Women Leaders in Technology