Honoring Our Past. Innovating Our Future.

Brennan P. Baybeck, CISA, CRISC, CISM, CISSP

Is chair of ISACA's Board of Directors and vice president of Security Risk Management for Global Customer Support Services at Oracle Corporation. In his role, Baybeck leads a global team that addresses IT security risk management for one of the largest lines of business at Oracle. He is also responsible for leading security, privacy and availability for customer-facing services, as well as Global IT's key enterprise IT services, including cloud initiatives. He has more than 25 years of experience in IT security, governance, risk, audit and consulting, and has worked in various industries designing, implementing and operating enterprisewide programs to address global security risk. He has held leadership positions at Sun Microsystems, StorageTek and Qwest Communications, and served as an information security risk consulting director for several years. Baybeck also has been actively involved with ISACA® for more than 25 years, serving many years as a chapter board leader and more than eight years working at the international level as chair for various working groups and as a Board director.

Q: As ISACA's incoming chair of the Board of Directors, how do you see ISACA® growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?

A: We have a number of areas on which to focus, including preparing ISACA constituents for the future and Industry 4.0. Engaging more enterprises and helping them understand the value that ISACA brings to the industry, their businesses and their employees, which will, in turn, help our members, is also a priority.

I believe ISACA has an important role to play in helping enterprises address big challenges such as IT governance, data governance and cybersecurity, which are more important than ever, as organizations drive digital transformation focused on adding value as quickly as possible to business using technology. We must also embrace the future of learning and knowledge platforms.

ISACA is in a unique position to really make people aware of the diversity challenges we have in the IT field. We have an opportunity to not only bring knowledge and understanding to this important challenge but also to be at the forefront of addressing this issue while helping solve the real business challenge of capability and skill set gaps in our industry.

There also needs to be a focus on making ISACA more relevant and valuable than ever to the constituents that we serve—members, chapters, enterprises, partners, government and industry.

Q: What in your past experience has best prepared you for this position on the ISACA® Board?

A: My executive experience at global technology, services and consulting companies has provided me with the opportunity to interface with various industry leaders, board members, executive teams and, most importantly, thousands of customers across the world, giving me great perspective and insight on how businesses strategize, innovate and operate on a daily basis. These experiences have allowed me to observe customer successes and how they achieved those successes, as well as their challenges and how they have overcome them (or not, which creates opportunities for ISACA).

I have worked in roles directly related to the areas that we serve for almost my entire career—cyber and information security, IT audit, risk management, and governance—so I have a very solid grasp of what provides value to our existing and future membership and the challenges that they face every day.

Q: What do you see as the biggest risk factors being addressed by IT security professionals? How can organizations protect themselves?

A: The speed at which our business customers are operating because they must. The IT organizations that we partner with are working with business partners who are driving significant and critical digital transformation activities to compete and, in some cases, to survive. When businesses are aggressively looking to dominate or struggling to survive, they are willing to accept risk that they may not have in the past. These decisions are creating new and significant security and IT risk challenges and, many times, these decisions are not informed, risk-based decisions.

Many of us may have traditionally focused on operational roles, which are important, but a real need of boards and executives is in the area of governance. In my experience, a properly informed board of directors or teams of senior executives always make the right decision for the business.

Q: You have extensive experience in executive leadership. How do you see the role of executives changing to meet the challenges of information security?

A: My experience has shown that executives are more informed about information security than ever, including at the board level. However, even though this is positive progress, we still have a long way to go. I am starting to see that security is no longer the number-one priority, mainly due to the various business transformation activities with which security is competing. When you think about it, it makes sense. If the business does not transform, it will no longer exist and its security will not matter. However, information security risk factors continue to grow due to those digital transformation activities. That being said, the biggest challenge for boards and executive leadership will be determining what is the proper balance of security risk vs. business risk. Yes, this is a challenge that has been around for a long time, but I think it is becoming more critical as security risk factors compete against business risk. Executives need to make sure the pendulum does not swing too far one way or the other.

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

A: Organizations need to think out of the box. Many are still hiring using legacy models focused on very specific skill sets and capabilities. The truth is that there are not enough of those "traditional" people to go around, so the more successful organizations are looking at other skill sets, capabilities and, more important, other demographic groups to fulfill their cybersecurity needs.

Organizations need to strongly consider leveraging partners. Savvy organizations are coming up with creative ways to integrate technology and services partners into their cybersecurity strategies and better utilize capabilities in those technologies to do more with less.

Automation, automation, automation. This will be a critical component of addressing the cybersecurity skills gap. Emerging technologies are already transforming the way we handle security risk and operations management today. These technologies will be a critical component in automating mundane but necessary security tasks and freeing up our most valuable security resources to do the most critical work.

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

A: A lesson that I learned a long time ago was assuming that my managers knew what my professional goals and objectives were and they were magically going to make those happen for me. It was a tough lesson to learn, as it caused me to miss a great opportunity for a promotion, but I learned it early in my career. What I learned is that those managers wanted to help me, but they did not know what I wanted or that I needed their help. You have to be in charge of your own destiny when it comes to your career. There are a lot of people out there who will help you and more resources than you could ever effectively use in a lifetime, but it is up to you to take the time to plan your career by creating professional and personal objectives; identifying the people, experiences and resources that can help meet those objectives; and then proactively executing on that plan.

1 What is the biggest security challenge being faced in 2019? How should it be addressed?

Data governance and protection. It has always been around, but some recent high-profile cases are bringing it to the forefront. Addressing it requires a top-down, executive-sponsored approach vs. trying to solve it simply with technology or from the tactical level.

2 What are your three goals for 2019?

- Capitalize and execute on strategic decisions and investments to expand ISACA's presence into the enterprise, emerging markets and government/public affairs
- Support and drive diversity initiatives
- Help ISACA's new chief executive officer (CEO) and his executive team be successful while strategically preparing ISACA for the future

3 What industry-related sources do you read on a regular basis?

- ISACA's knowledge resources
- *InformationWeek Dark Reading*

4 What is your favorite benefit of your ISACA membership?

The leadership, professional and personal development opportunities that ISACA provides to its members

5 What is your number-one piece of advice for IT security professionals?

Always be curious, ask a lot of questions and, most important, be a life-long learner. The security field is constantly changing, so being a lifelong learner drives new ways of thinking, fresh perspectives, creativity, innovation, a solid grounding, and, of course, helps keep your mind young.

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

I am an avid outdoorsman and love to do anything outdoors. I love to share my passion for the outdoors with my wife and my two awesome kids. My favorite activities are fly-fishing and bird hunting, both of which involve being outdoors in some of the most rugged, beautiful and peaceful places in the world.