Building Tomorrow's Leaders, Today

Rob Clyde, CISM

Is chair of ISACA's board of directors, executive chair of the board of directors for White Cloud Security (trusted app list enforcement), and independent board director for Titus (leader in data protection, categorization and classification). He is the managing director of Clyde Consulting LLC, which provides board and executive advisory services to cybersecurity software companies. He serves as an executive advisor to HyTrust (multicloud workload security) and BullGuard Software (consumer and smart home cybersecurity). Prior to becoming chair of ISACA's Board of Directors, he served as vice-chair, chaired the board-level ISACA Finance Committee, and served as a member of ISACA's Strategic Advisory Council, Conference and Education Board and the IT Governance Institute (ITGI) Advisory Panel. Previously, he was chief executive officer of Adaptive Computing, which provides workload management software for some of the world's largest cloud, high-performance computing and big data environments. Prior to founding Clyde Consulting, he was chief technology officer at Symantec and a cofounder of Axent Technologies. Clyde is a frequent speaker at ISACA events, cybersecurity conferences and for the US National Association of Corporate Directors (NACD). He is an NACD Board Leadership Fellow. He also serves on the industry advisory council for the Management Information Systems (MIS) Department of Utah State University (USA).

Q: You have served and currently serve on a number of organization boards and as an executive advisor to some cybersecurity companies. What in your past experience has best prepared you for the role of ISACA board chair?

A: Currently, I work with several different organizations as an executive advisor to the chief executive officer (CEO) or as a board director. As a board director, I carry out the fiduciary, governance and strategic leadership responsibilities that are inherent in that role. I consider myself a team member of each of my clients. I work closely with the CEO, board directors, other executives and staff. In the case of ISACA, I provide a similar service as a board director and chair, but *pro bono*.

I really enjoy this because I have the privilege of simultaneously being on the teams of several great organizations and the satisfaction of making a significant difference to their success. My executive advice may cover any area of the business, including governance, strategy, organization positioning and messaging, product strategy, product road maps, improving development velocity and quality, mentoring leaders, helping to identify inventions and file patents, sales, support, professional services, organization structure, and mergers and acquisitions.

A long list of experiences has prepared me for this role. Here are a few highlights: initially built my technical skills as a programmer writing information security products, since led development and product teams, led business units, served as the chief technology officer (CTO) for Symantec, and as a CEO. Through ISACA I was able to hone my cybersecurity skills and better understand audit and risk functions by attending and speaking at ISACA events at both the international and chapter level.

What may be less obvious are the failures and adversity I faced that helped build character and understanding. For instance, early in my career, one of my software products crashed all of the systems for a well-known sports league during a proof of concept and I was kicked out of the building and asked to never return. I did not give up and continued trying to improve the product.

Later, out of that company, I cofounded Axent Technologies, which focused on enterprise information security. It grew exponentially and was ultimately taken public and purchased by Symantec. During this time, my wife was struggling with cancer and eventually passed away before we sold the company. While her illness and passing were incredibly traumatic for me and my children, learning how to deal with adversity and loss gave me more empathy for others and an ability to focus on what is truly important and not sweat the little stuff.

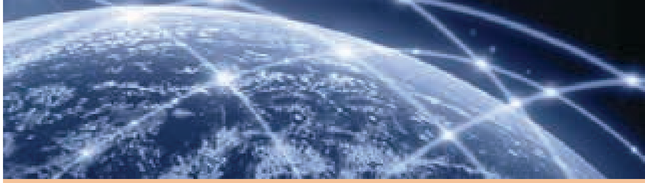
Q: What do you see as the biggest risk factors being addressed by information security professionals? How can organizations protect themselves?

A: Ransomware attacks continue to increase rapidly. In 2018, we are seeing more targeted ransomware attacks with higher ransom demands. Not just Windows systems are being targeted, but also Linux systems, Mac systems, smartphones and IoT devices.

To deal more effectively with this risk, organizations should consider bolstering their current approach by adding next-generation white-listing tools that allow only trusted code to run. Organizations can choose how tightly to lock down that list.

Privacy also remains at risk, as made evident by the GDPR, which describes many beneficial actions such as discovering, categorizing and encrypting personal data.

Lack of sufficient cybersecurity practitioners poses a risk that organizations may not be able to execute well on their security strategies and effectively detect and respond to incidents. Dealing with the cyberskills gap is a challenge that leaders must navigate.



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: Meeting the challenges of cybersecurity will require strong leadership including from the board, the CEO and the C-suite. In fact, organizations do not just need cybersecurity, they need cyberresilience, which includes the need for security, but also high availability, scalability, and the ability to allow an organization to keep running in the face of attack or disaster.

The role of executives relative to this is changing as organizations view cybersecurity and resilience as not just issues to be delegated to chief information officers (CIOs) and chief information security officers (CISOs), but as fundamental to the health and growth of the business. The CEO must provide leadership and make cyberresilience, including security, something that is planned, tracked and regularly discussed at executive meetings and at the board level.

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

A: Today, most organizations try to hire talent from other organizations. This is difficult and there are not enough cybersecurity professionals available to fill all open positions. To deal with this in the near term, organizations should consider cross-training existing employees or new hires in adjacent areas such as network or systems administration. This can include having them train for and pass appropriate certifications to demonstrate their knowledge and skill. Organizations should drop requirements for a four-year college degree and consider applicants who have been trained at technical schools, in the military or have otherwise demonstrated aptitude. They can use intern programs as a way to mentor and encourage future candidates to gain experience in the field.

In the longer term, we need to work with students from the moment they enter secondary school and at the technical school, college and university levels to encourage more students to go into technical fields such as cybersecurity. We also need to encourage and support more women entering the field. Today, women make up only about 11 percent of the cybersecurity workforce (according to the Executive Women's Forum). I am an enthusiastic supporter of ISACA's SheLeadsTech program as a way to do this. In addition, ISACA's State of Cybersecurity 2018 Report clearly showed that having a diversity program dramatically closes the perception gap between women and men as to equal advancement opportunities in the cybersecurity field.

Q. How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when recruiting new members of your team?

A. I started my work in programming and cybersecurity before certifications ever existed. So, by the time certifications appeared on the scene, I was fortunate enough to be well established in the field. Nevertheless, I was one of the very first to receive ISACA's Certified Information Security Manager® (CISM®) certification and have been vigilant to continue my education and keep it current. It is important to me to continually learn and the goal of earning continuing professional education hours (CPEs) to maintain a certification helps me to do that.

The Certified Information Systems Auditor® (CISA®) certification has become a requirement for most IT audit positions. I also think that performance-based certifications such as ISACA's CSX Practitioner (CSXP) are the way of the future for cybersecurity since employers are looking for candidates who can demonstrate hands-on experience.

1 **What is your favorite blog/online content?**
ISACA's *The Nexus* (of course).

2 **What is on your desk right now?**
Nothing, except my notebook and iPad. I believe in being entirely paperless and do everything electronically. I am encouraging ISACA and its members to go paperless as well. I travel frequently and, since my office contents are electronic, I take my desk with me wherever I go.

3 **What are your goals for 2018?**

- Make ISACA even more relevant and valuable to our members, profession, industry and enterprises, including continuing to innovate with our training, certifications, the CSX platform and new CMMI Cybermaturity Platform.
- Provide strong board leadership demonstrated by great governance, execution oversight and strategic plans.
- Develop and execute on a plan for an ISACA charitable foundation.
- Listen, learn and act.

4 **What is your number-one piece of advice for technology professionals?**
Participate. Volunteer—starting with your ISACA chapter and then at the international level. Look for opportunities to contribute. When you do this, you will grow much faster as a professional, gain valuable skills and insights, build your network, and feel like you are making a difference.

5 **What's your favorite benefit of your ISACA membership?**
Networking. I thoroughly enjoy interacting with ISACA members at various events and chapters all over the world. ISACA is more than just a professional association, it is a global family.

6 **What do you do when you are not at work?**
After losing my first wife, I married a wonderful woman, Becky. We just celebrated our 19th anniversary and together have six children and 17 grandchildren. So, my favorite thing to do is spend time with my wife, children and grandchildren. This often includes boating, fishing and swimming, which we love to do.