Driving Digital Transformation

Gregory Touhill, CISM, CISSP, Brigadier General, United States Air Force (ret.)
Is the director of the CERT Division at the Carnegie Mellon University Software Engineering Institute (Pittsburgh, Pennsylvania, USA). He is also a professor of cybersecurity at Carnegie Mellon University's Heinz College. Prior to joining the CERT, he served as President of Appgate Federal, a cybersecurity and secure remote access company. Touhill has extensive experience as a director of profit and loss corporations and nonprofit organizations, including serving on the Splunk, Intel and Symantec Federal Advisory Boards. Prior to entering the private sector, Touhill concluded a distinguished career of public service culminating in his selection by the President of the United States as the US government's first chief information security officer. His other civilian government service includes duties as the deputy assistant secretary, cybersecurity and communications at the US Department of Homeland Security, and as director of the US National Cybersecurity and Communications Integration Center, where he led national programs to protect the United States and its critical infrastructure. He is a retired US Air Force general officer, a highly decorated combat leader, an accomplished author and public speaker, and a former US diplomat.

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

A: Information technology is changing the world. It is transforming how we interact, learn and communicate. Around the world, IT fuels national prosperity and security, and ISACA members are at the forefront of optimizing and securing the digital ecosystem. The digital ecosystem is constantly changing and so is ISACA. My fellow members have seen the improvements we made to our digital presence in the last year, including a great new web presence, improved digital content, and expanded training and certification options. Looking ahead into the coming Board year, we will continue our digital transformation with new content and capabilities we hope delight our fellow members.

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

A: First, I am and have been an ISACA member. I proudly maintain my Certified Information Security Manager® (CISM®) certification and look at my Board service as focused on making our organization better. Second, I have a rich professional experience base that has taken me from the server room to the board room. Third, my professional experience has yielded a global perspective. I have been fortunate to have lived in and on several countries and continents and have visited 45 countries (and counting!).

ISACA is a global community, and our diversity makes us strong and vibrant. I have been a US Air Force general, the chief information security officer (CISO) of the United States government, the president of a successful cybersecurity start-up, a professor at Carnegie Mellon University, and a member of numerous BoDs of large and s mall organizations. Serving the ISACA community is part of my professional DNA.

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

A: I see three major risk areas with which we ought to be concerned. The first involves security and privacy. I believe that to have privacy, you ought to have strong security, and *vice versa*. There is a wide range of threat actors who seek to gain a competitive advantage by compromising our security and privacy through unauthorized access to our data. Second, transformation to the digital ecosystem continues to move forward at an amazing pace. To survive and thrive in the ecosystem, you have to stay up to date. I advise my students that means that just as you have to keep your hardware and software properly patched and configured, with the latest updates, so do you have to keep the "wetware," we the humans, properly patched and configured, too. Finally, having easy access to best practices and experts to help you identify and manage your risk is vital.

I view our global ISACA community as a force multiplier for our members, giving them access to best practices from around the world in all critical infrastructure sectors. By exercising due care and due diligence in cybersecurity, privacy, and investing in optimizing your people and processes, world-class organizations are minimizing their risk and thriving.

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

A: I believe that nearly every business or organization is reliant on IT. Whether they recognize it or not (and most executives do), they have become data-driven enterprises. As a result, if you aspire to be an executive in today's marketplace, you need to ensure that you have the requisite literacy and understanding of the digital ecosystem to drive value and growth in your business. Protecting your data is an existential requirement for organizations. I am seeing more and more BoDs and executives attending formal executive education courses to enhance their ability to make informed decisions on cybersecurity and risk. I am heartened by the recognition in board rooms around the world that cybersecurity is an essential element of corporate success. While many organizations are playing catch up regarding security, it is now at the top of the corporate agenda and I expect it to stay there.

Q: What do you think are the most effective ways to address the skills and gender gaps in the technology space?

A: Great organizations clearly identify their visions and the strategies to achieve them. They develop plans to support strategies and identify mission-essential functions and the underlying tasks needed to fulfill them. They do not stop there. They identify the skills needed to execute the tasks and ensure that they have the right people, at the right time, with the right skills and experience to achieve their goals and objectives. I find that many organizations have not yet successfully followed that construct or are unable to recruit and retain people with the requisite skills to meet their mission-essential tasks.

While many organizations try to fill the gaps by offering enhanced salary and benefits, many are successfully improving their position by investing in reskilling and upskilling their workforce. Forecasting skills gaps before they happen reduces risk and gives the organization time to take proactive actions, such as reskilling and upskilling, to round out your team. I am also a huge proponent of programs such as internships that promote the development of new personnel joining the workforce. Finally, I am convinced that diversity makes us better and recognize that gender gaps exist in the technical workforce. Women are underrepresented in the cyber and technology workforce. I am convinced that when we attract women to the technology fields, we will boost our productivity, quality of work and erase the personnel shortages people cite in the technology community.

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 am a firm believer that certifications matter and are a measure of aptitude, potential and motivation. When I assess candidates, I look for certifications they have attained. Many people earn certifications on certain products, yet if I am looking for someone to lead a team, to improve a process, to conduct audits and assess risk, or evaluate disparate technologies, I am looking for more. I am looking for professionals who are serious about their careers who have gone the extra mile and have earned certifications that enhance not only their current jobs, but their future jobs. That is why, when I was in government and military service, we identified ISACA certifications and other certifications as key requirements when we were creating the cyberworkforce career path.

1 What is the biggest risk challenge being faced in 2021?

I believe that cyberrisk areas associated with remote work are the greatest risk. Malicious actors are actively hunting persons and organizations leveraging phishing, attacks on personal devices and services, and leveraging weaknesses in unpatched or misconfigured virtual private networks to gain access to valuable information and data.

2 What are your three goals for 2021?

- Safely emerge from pandemic restrictions and resume in-person ISACA events where it is safe and prudent to do so
- Publish an updated ISACA strategy
- Provide clear guidance and oversight to the executive team as they work to complete the current digital transformation activities

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

- *ISACA SmartBrief on Cybersecurity*
- Krebs on Security
- OODA Loop
- *Wired*
- *TechRadar*
- HSToday

4 What is on your desk right now?

Four computers, a cup of tea that desperately needs a refill, a printer and a leg lamp (it is a major award!)

5 What is your favorite benefit of your ISACA membership?

The ISACA community. Everywhere there is an ISACA chapter, you have a friend.

6 What is your number-one piece of advice for cybersecurity professionals?

Do not forget cybersecurity is a risk management issue centered on people, process and technology. Do not focus solely on the tech.

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

Whatever my wife asks me to do.