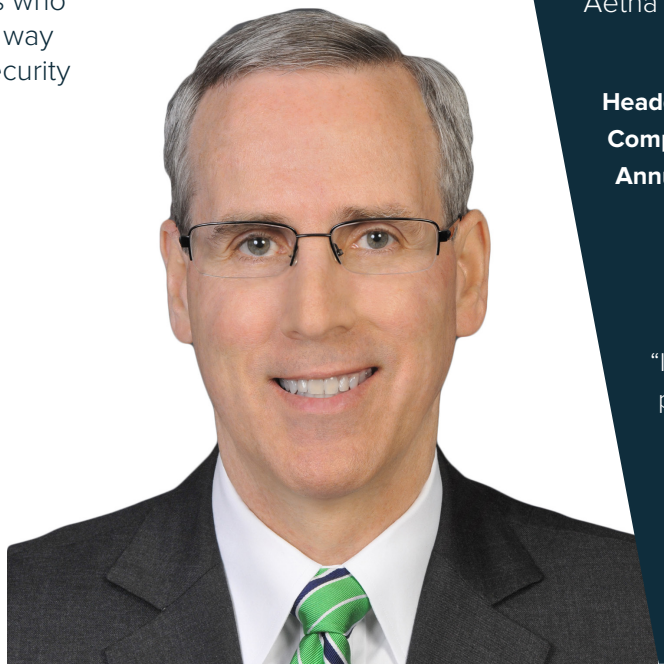
PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs



JIM ROUTH

CISO
Aetna

Headquarters: Hartford, CT
Company size: 49,000+
Annual Revenue: $58 Billion

"It is important to share information on your practices. I take calculated risks in order to manage risk and by sharing this, I not only enable the industry to improve their capabilities, but I receive validation of what I am doing and feedback to see if I'm on track."

Jim Routh is a known name in the industry; between his contributions to numerous news articles and many high-profile speaking engagements, his drive to share information on practices and continue to improve the industry is evident. Currently the CISO at Aetna, Routh leads his team with clarity, openness, and purpose, creating an environment of continued growth and success.

THE POWER OF KNOWLEDGE-SHARING

On Routh's first day as an official CISO, he was working at American Express and encountered a situation that demonstrated the power of connecting with other CISOs. Routh saw a meeting on his calendar calling for a presentation on Information Security Strategy to the OCC (Office of the Comptroller of the Currency). Since Routh was new to the CISO role, he called upon Steven Katz (the first ever CISO) to help guide and instruct him on developing a strategy. Within an hour and with no previous relationship, Steven arrived with two other financial services CISOs, all of whom dropped everything to aid Routh in formulating the presentation and practicing his delivery. Routh says, "They taught me a valuable lesson, a lesson that I still pay attention to today - which is - the right thing to do is help each other in order to make the industry more resilient. That means making some sacrifices for the good of others."

With many years of experience under his belt since his first day at American Express, Routh now mentors and communicates with other CISOs on a regular basis. "There is a very common bond that is established, because when there is a major breach or a publicized attack, most of the time we already know about it, we know the trade craft, and often who the threat actor is. If we don't know right away, we get that information from people who we have trust-based relationships with," says Routh.

Routh spends time mentoring first-time CISOs, who often come directly to him for advice. This advice includes how to organize the security department, talk to the Board,

"Everyone should adopt a framework for their security program; my only caution is that frameworks alone don't stop sophisticated threat actors. There is a flurry of activity today to try to adopt and implement standards. Aetna chose to implement both the NIST Cyber Security Framework and the NIST 800-53 Standard. Adopting standards is positive for the industry and should be pursued. The trigger events are major public breaches by nation-state sponsored threat actors. Although the frameworks represent good, solid information security practices and should be pursued, more is necessary to deal with highly sophisticated threat actors. Changing the game for the adversary requires an in-depth understanding of their tactics from cyber security intelligence sharing and the use of "game-changing" control design that is innovative."

deal with business stakeholders, threats that are likely to impact them, and a multitude of further pressing concerns. In reality, Routh states that the hardest and most important decision that CISOs make every day is how to allocate resources to the highest risk. Every CISO has it in their best interest to do this, but it is a challenging thing to do because you have to constantly make trade-off decisions.

RECIPE FOR A SUCCESSFUL TEAM

Without a question, Routh wholeheartedly believes in the Professional Development Plan that is established within his security organization. This program allows each member of the security team to choose two skills or competencies that they would like to master, and they are provided with opportunities throughout the year to achieve this. "My job as a leader is to provide an environment that gives them what they need in terms of their professional development, and ultimately I want them to have the opportunity of choice or to have options available to them. We match their desire to invest in a skill or competency with development activities, in some cases adjusting their role to help them learn what they would like to master," says Routh. One trend Routh notices is his team picking a technical skill and a soft skill, such as choosing how to be an effective communicator along with learning how to interpret results from static analysis tools for application developers.

Paired with an extremely talented team, Routh has invoked a risk-based approach to running the security program. He shies away from a program geared only towards compliance, but one that focuses on understanding risk in order to make pivotal decisions in relation to allocating resources to the highest risk. This risk-based approach is transparent throughout the organization, resulting in a robust preparedness for security threats and vulnerabilities. This risk based approach to security works hand-in-hand with a robust privacy program, which is essential in a health care organization.

CYBER SECURITY LEGISLATION

The United States House of Representatives is taking up cybersecurity legislation which could grant companies protection from legal liability if they choose to voluntarily share certain cyber threat data with the government. "The basis for the proposed legislation is a problem long known by lawmakers to address constraints to sharing cyber security intelligence back and forth between federal agencies and the private sector. The information sharing capability needs to be facilitated to address two things. First, there must be sharing of threat intelligence from different federal agencies with the private sector. Second, it must encourage more free flow of cyber intelligence and information from the private to the federal sector and for those respective agencies to have the ability to do something with that information."