The Role of the CISO

An Interview with
Jim Routh, Chief Security Officer, Aetna

EDITORS' NOTE *Jim Routh has held his current post since May 2015. He is also a board member of FS-ISAC, as well as Chairman of the Board of National Health ISAC. Prior to this, he held roles including Global Head of Application, Mobile, and Internet Security, JP Morgan Chase; Management Consultant, Emtec Global Services; Community Chairman, Archer Technologies; CISO, KPMG; Chief Information Security Officer, Managing Director, Depository Trust & Clearing Corporation; CISO, American Express; VP Information Risk Management, American Express; VP Information Technology, American Express; VP, American Management Systems, Inc.; and Director, DMR Group, Inc. He received his B.A. in History from Hobart College.*

Jim Routh

COMPANY BRIEF *Aetna (aetna.com) is one of the nation's leading diversified healthcare benefits companies, serving an estimated 46.3 million people with information and resources to help them make better informed decisions about their healthcare. Aetna offers a broad range of traditional, voluntary, and consumer-directed health insurance products and related services, including medical, pharmacy, dental, behavioral health, group life and disability plans, medical management capabilities, Medicaid healthcare management services, workers' compensation administrative services, and health information technology products and services. Aetna's customers include employer groups, individuals, college students, part-time and hourly workers, health plans, healthcare providers, governmental units, government-sponsored plans, labor groups, and expatriates.*

How important is it that the CISO role be given a seat at the executive table?

Having a CISO at the table is becoming not only a common practice but an essential one. There is a whole series of contributing factors to that. One is technology intensity meaning that technology as an enabling capability is far more concentrated in consumer businesses and to some extent in B-to-B tranactions, so this technology is more of a variable.

The consumerization of technology has fundamentally changed enterprise computing architecture as we move to cloud computing and distributes user-driven computing on a mobile platform.

Obviously the implications from a cyber control perspective are far more significant and require more innovation to come up with capabilities that protect data when individual devices are used, where cloud services are hosting that data, and where consumers or client institutions are provided access to that data or are providing that data.

There is a shift in that the understanding of emerging technology is becoming a critical part of the skill that is required for overall technology competence. Understanding how technology evolves and how emerging technology and start-up technology influences how consumers interact are now vital and essential for a CISO. An overall understanding of how IT is managed and works in the business is probably less of the determining factor of success for a CISO than learning to communicate with senior business leaders and understanding the implications of the business strategy. A CISO has to articulate a business architecture that has a control element embedded in it and that, in some cases, is part of the value proposition that a consumer sees.

Softer skills are becoming more of a premium for the chief information security officer. Technical skills alone will, in many cases, be a constraint and limitation in terms of the CISO's ability to influence and change the business.

How critical is it to communicate effectively with the board when you often speak different business languages?

It's vital. I've chosen to introduce the board to basic terminology as part of an educational seminar each year on cybersecurity, which includes issues like threat actor, tradecraft, threat landscape, and nation state.

Primarily I speak in terms of impact on revenue, on cost, and on brand since 70 percent of IT security controls fall under the banner of improving quality or providing efficient and effective capability at a reasonable cost. I often try to avoid falling into a trap of determining what the probability of risk is and quantifying that to justify an investment decision.

Putting cybersecurity investment into the context of business decision making every day is the right way to go and needs to be a core capability of the CISO. When they have that, it's easy to talk to the board and senior leaders.

You also serve as Chairman of the National Health ISAC. Will you talk about the role ISACs play?

The most common question that is triggered when any kind of cyber threat impacts an organization or an enterprise is: Is that threat targeting the enterprise or targeting specific employees or customers of the enterprise or is that threat impacting the entire industry?

As threat techniques or tactics evolve, understanding whether or not it is a targeted attack on an enterprise is the most basic question of the information risk professional.

The most effective way of answering that question in real time is to reach out to other enterprises and other security professionals and ask if they are seeing it too.

If it's a targeted attack, this engenders a different response as techniques are predicated on whether it's an opportunistic or targeted attack. That is the question that gets answered through an ISAC. It's the most basic and fundamental question that gets asked almost every day. The ISAC will enable communication channels to share information and answer that question.

It gets more mature than that. Cyber criminals are shifting tactics because stolen personal information, including social security numbers, are available to them through the black market. They could buy that information and could use it to commit fraud. The information on the tactics used is vital to enterprises within the same industry vertical, and the ISAC provides many vehicles for sharing that information broadly.

By having access to that information, I can use it to make Aetna more resilient to those attacks. I know the tactics that are being used and can share information about controls that are effective against those types of attacks with other industry players to make them more resilient.

The ISACs representing different industry sectors are the lifeblood behind different vehicles for communicating and sharing information. As technology emerges, evolves, and matures, and as businesses change, the need for that level of interaction is highlighted and grows.

ISACs have been around for over 15 years. The practices are mature and well established, and I use and benefit from them more so today than 15 years ago. ●