# Is the Knowledge Transfer Gap Hurting Security?

By Bob Hayes

By Kathleen Kotwica

Adding business value. Getting a seat at the table. Running security like a business. Aligning security with the organization. These are the contents of the Holy Grail of security leadership. Everybody talks about them. Everybody wants them. But most security leaders view them as the stuff of legend – great for motivation, but unattainable in reality.

The industry as a whole has a grasp on the issues and many organizations have worked in recent years to help security leaders develop individual skills that get them closer to these goals, step by step. There is an abundance of magazine articles, certifications and seminars with that aim, and industry associations continue to partner with business schools to help security leaders better understand business. Still, few manage to capture the designations of "business enabler," "executive influencer," "security aligner." What's missing?

Business schools and industry business programs are perhaps the most useful existing resources pointing security leaders in the direction of success, yet they leave out an important element. Taught by business professors, they focus on helping security leaders understand business practices and speak the business language. But these programs fail to continue to the next stage: How do they marry business processes with the job of risk mitigation? How does security become a business unit in its own right?

Knowing how to talk business doesn't equate to an automatic understanding of how security adds value. It doesn't give security professionals the practical programs to implement to support the business. Like any other business unit, security must follow a process to attain true management support and align with business. This process includes documenting work efforts to show what security is actually doing on a day-to-day basis. It includes the often arduous task of meeting with all key executives of the business units to find out their plans and to discover the role security can play in their goals. It also entails holding business unit leaders accountable for their decisions on what risks are important to mitigate and at what level. This is the type of knowledge that has allowed the few truly aligned security leaders – people like those who will appear in this magazine's Most Influential list next month – to reach their level of influence and success. But where do you learn how to do this?

Research conducted by the Security Executive Council has identified seven personas that most security leaders generally fall into. One of the first steps to learning how to move up this continuum is finding out which category you're in.

- Those new to security or new to their industry
- Those interested in learning the other side (an IT leader learning corporate security or vice versa)
- Program creators/validators, who are creating or recreating programs due to changes in corporate leadership or strategy
- Program facilitators, who have established security programs at a maintenance level, generally with limited resources
- Urgent innovators/expanders, who have established programs and are responding to significant situations, yet looking toward emerging issues
- Program expanders, who are expanding on existing boundaries and roles of security, thus advancing internal business alignment
- Next-Generation Leaders, who are working at an industry or national level. These individuals are rare. They are future oriented and work across many domains. They are aligned and are influencers in their organizations.

Many of the elite individuals who have reached Next Generation status are Tier 1 Security Leaders™ in the Council, but they make up a very small segment of current security leaders. We've spoken with them about how they reached their level of success, and in most cases it comes from a combination of understanding the corporate culture, organizational readiness, personal ingenuity and motivation, mentorship, strategic thinking and great timing. Yet one of the questions we frequently hear from even these top-tier individuals is, "How do I teach my people to be more strategic?" Reaching a state of influence and alignment doesn't in itself give a person the ability to show someone else how to do so, and often at this level there is little time to show others how to get there.

Thus, there is a wide gap in the transfer of valuable knowledge to security leaders, and this gap is dangerous. It means that the rare organization that now has a Next Generation Security Leader in place may have to begin nearly from scratch once that individual retires, because no successor has been able to grasp the secrets to his or her success. It means that when the industry loses one of these few, it has to start over every time and simply wait for the next visionary to show up. It means our industry will never move forward.

The Security Executive Council has a roadmap that will help us fill this knowledge transfer gap. Next month in this space we'll start discussing what the industry can do. SECURITY

**About the Columnists:**

Bob Hayes is Managing Director of the Security Executive Council. He has more than 25 years of experience in security, including eight years as the CSO at Georgia Pacific and nine years as security operations manager at 3M. Kathleen Kotwica, PhD, is EVP and Chief Knowledge Strategist for the Security Executive Council. She develops strategies and processes to identify, store, understand, build upon, and disseminate the Council's Collective Knowledge™ and insights.. To learn about becoming involved, or to offer comments or questions about Next Generation Security leadership, e-mail contact@secleader.com or visit https://www.securityexecutivecouncil.com/sm.