SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Addressing the Knowledge Transfer Gap

Bob Hayes and Kathleen Kotwica, Ph.D.

Originally Published in Security Magazine

Last Updated December 2016

Addressing the Knowledge Transfer Gap

Created By: Bob Hayes, Managing Director and Kathleen Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council (SEC)

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 leader 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 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.

1. Those new to security or new to their industry

2. Those interested in learning the other side (an IT leader learning corporate security or vice versa)

3. Program creators/validators, who are creating or recreating programs due to changes in corporate leadership or strategy

4. Program facilitators, who have established security programs at a maintenance level, generally with limited resources

5. Urgent innovators/expanders, who have established programs and are responding to significant situations, yet looking toward emerging issues

6. Program expanders, who are expanding on existing boundaries and roles of security, thus advancing internal business alignment

7. 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 SEC, 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.

Seven Characteristics of a Knowledge-Sharing Program So what is our industry to do? If we can’t address this gap, the practice of security can never move forward. Without the right training in place, every time a visionary security leader retires, his or her replacement has to start anew instead of building from the level of his predecessor.

Successful security executives are not going to be able to individually mentor every security and risk practitioner who wants to learn their secrets. We need a new breed of training program that can pass this knowledge along. We believe there are seven criteria this new type of knowledge-sharing program must meet.

1. It has to have the right teachers. Business professionals do an expert job of teaching business theory and practice, but a course cannot adequately address how risk mitigation should work within the business unless it offers equal instruction from individuals with personal experience in the security and risk fields. Our industry needs a program that is taught by business and security professionals, not business or security professionals.

2. It has to be developed with input from practitioners. It’s true that sometimes we don’t know what we don’t know. But many security practitioners are very clear on the type of knowledge they need and the

type of training they're not finding. An effective program will solicit input from the people on the front lines to inform the curriculum.

3. It has to cover the subjects Next Generation Leaders must master. As we explained in our last column, Next-Generation Leaders are those rare individuals, working at an industry or national level, who are future oriented, who work across many domains, who are aligned with the business and who are influencers in their organizations. While input from practitioners is one important aspect of curriculum development, it's also crucial that this new breed of program offer a curriculum that is built from a distinct and intimate understanding of the skills, characteristics, and processes that help make our most successful colleagues so successful.

4. It has to begin by assessing each participant's leadership development and needs. A course can't teach you how to move forward if neither you nor the instructors know where you are now. In last month's column we described seven personas into which most security leaders generally fall. An effective course curriculum will begin by asking participants to think about and try to understand where they are in their organization, in their career path, and in their leadership development so that they can better understand what they need to learn.

5. It has to guarantee that it will provide actionable information. It's great to know how to talk the business talk. Now what are you supposed to do with that? That's the problem many existing programs have. A program that truly and effectively teaches "the business of security" will be one that gives participants tangible takeaways they can immediately begin to use in their organizations.

6. It has to allow participants to continue to connect after the coursework is over. Schoolteachers joke (some more seriously than others) that their participants always come back from summer vacation having forgotten everything they learned the year before. Once a class is over, it can be easy to go back to the grind and forget what you've been taught. An effective program will offer ways for participants to stay connected to the coursework after it's over by continuing to communicate with instructors or fellow participants.

7. It has to be affordable. The tuition for business school offerings can run into the tens of thousands, and in this economy even profitable multinational companies are balking at those prices. If a new training program is going to change our industry, it has to reach a lot of people, and the only way to do that is to make the program extremely affordable.

At the Security Executive Council, we want to see our industry transformed. We want to see a program that offers everything we've described here, because we think this type of training could help to elevate security to an executive concern across the board.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com