Creating the Information Security Village

By David Lam, Kimberly Pease, Stan Stahl and Kurt Takamine

Security must now be completely and fully integrated into the daily lives of business practitioners just as it is now a passionate part of the daily lives of security professionals.

Twenty-five years ago, Information Security was something the big guys – government, banks, aerospace companies, and large insurance companies – were concerned about. Networking was in its infancy and the security perimeter was relatively easy to define. Threats in that bygone era were largely confined to spy agencies of foreign governments and insiders.

In those two and a half decades, the world has changed drastically. Threats now come from anywhere – both inside and outside the organization. A cybercriminal anywhere in the world threatens sensitive information wherever it resides. A lively black-market in social security, credit card, and bank account numbers, as well as other information easily converted to cash, has spawned a cyber-subculture making loads of money controlling botnets, sending virus-laden spam, writing Trojan horses, phishing, pharming, and selling zero-day exploits.

In today's world, everyone is at risk from cybercrime. And, it will take us all to lower the risk to acceptable levels. Information Security no longer simply involves those working in the field as professionals. Today everyone must participate in lowering the risk. Every IT manager, IT vendor, CIO, CTO, CFO, COO, CSO, and CEO; every member of every board of directors; every employee, whether in IT, purchasing, audit, sales, or HR, must be a part of the Information Security solution. Every computer user has a role to play in lowering the community's information risk. We security professionals cannot secure our organizations by ourselves.

Security must now be completely and fully integrated into the daily lives of business practitioners just as it is now a passionate part of the daily lives of Information Security professionals. We have an imperative to create a community that has an Information Security mindset, understanding that computer assets must be innately secured, just like we now understand that we must lock the front doors to our houses.

We must, as advocates of Information Security, create an *Information Security village* – a set of communities that understand that an Information Security mindset is not optional; it is required for business survival. The implications of this simple fact – that it takes the village to secure the village – are vital. It is our responsibility as Information Security professionals – and ISSA members – to provide our expertise, guidance, and especially our wisdom to the broader community. This is not a new responsibility, but one that flows from the very essence of our profession. Consider the following from the Information Systems Security Association website, for example:

> *The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.*[1]

The ISSA Code of Ethics[2] states that we are to "promote generally accepted Information Security current best practices and standards." The ISSA International Ethics Committee[3] instructs us to *include broader audiences in meeting Information Security needs*. And, the current draft of the GAISP[4] says we are to "be an authoritative source for opinions, practices and principles for information owners, Information Security practitioners, information technology products, and information systems." Common sense tells us the same thing: If people do not know what is required to protect information, then they will be unable to protect the information for which they are responsible.

It is time that we, as security professionals, step up as leaders and advocate the need for Information Security in every part of life. We must evangelize the need for Information Security, teach others, and bring them into our fold. As Information Security professionals and ISSA members, we are responsible for creating a total Information Security Culture, the Infor-

1 http://issa.org/Association/ISSA-Profile.html
2 http://issa.org/Association/Code-of-Ethics.html
3 www.issa.org/Downloads/ISSA-Ethics-Presentation-20070427.ppt
4 Generally Accepted Information Security Principles, GAISP V3.0

mation Security Village, if you will, in which everyone shares responsibility for securing our sensitive information.

Dr. Peter Senge, MIT professor and author of *The Fifth Discipline*, can provide some applicable insights here.[5] First, *leadership springs from deep, personal convictions*. ISSA members need to see creating the Information Security Village as a top priority, not just rhetorically, but practically, as well. To truly see this change, we must embrace this cultural challenge as a critical success factor of our raison d'etre. In Senge's terminology, we must "change the mental model" of our colleagues so that they see their Information Security responsibilities as something that really makes a difference.

To do this, we must communicate our assumptions and values succinctly and constantly. Part of our responsibility is to educate the non-technical community around us. If others outside of our organizations (e.g., CEOs and other non-technical leaders) cannot understand and build upon our assumptions, cultural change in the village will not occur.

We also need to help our colleagues anticipate the next curve. Cybercriminals are always one-step ahead of the game. To survive, they must be proactive. To defeat them, we must be two or three steps ahead of them. In essence, we must think like these hackers.

We have to get the people we work with to feel the same way. Most organizations are involved in what Senge labels *adaptive learning*; that is, dealing with the problems that present themselves to merely survive the current crisis. We need to help our village become generative learners, so they may spontaneously make the right decisions when confronted with a new or unfamiliar situation.

We must help our colleagues learn to see the forest *and* the trees. Leaders are tasked with seeing the big picture, and being able to understand the broad concerns and consequences of those observations. But, they must also be able to see the key details as well. The difference between effective and ineffective leaders is that the former are able to discern which details are critical to the solution.

We need to assist our colleagues in developing a forest-like perspective about Information Security and in understanding the specific information security trees that connect to their job responsibilities and threat profiles. Only in this way will they be able to become the generative learners we need them to be.

CIOs, CTOs, IT managers, and IT vendors, for example, need guidance in securely implementing critical systems. CEOs, CFOs and Audit Committees need guidance in understanding the true risk to their financial and other information systems. Parents, too, need guidance in meeting the safety and security risks that their children face. In order for each group to effectively support the community's security, it must understand its own Information Security trees in the context of a deeper understanding of the entire forest.

Smaller organizations face their own special challenges. In small organizations, IT managers often serve as the Chief Information Security Officer (CISO). In even smaller companies, the entrepreneur is the CISO. They may not know that they serve as the CISO, but they do. And, without our assistance, they are struggling without the wherewithal, understanding, or corporate weight to properly secure their systems.

Here is a story that helped us understand the importance of helping people get their arms around the challenge. One network manager was extremely skeptical of newly-implemented security policies. However, when he came back from ethical hacker training, his first words were, "you can't believe what they can do!"

This must be our starting point: to assist those who do not yet see; to open their eyes to the ease with which cybercriminals can take over systems; to assist them in shifting their position from the prevailing naive belief that they are secure to the deeper recognition that they are not. And, having opened their eyes, to provide them with the tools, the practices, and the wisdom, so they can do their part in securing the village.

The time has come for Information Security professionals everywhere – and ISSA members in particular – to reach out to our business peers and communities and advocate with deepest conviction, evangelize constantly and succinctly, and take advantage of learning moments. We must help them learn firsthand the critical role we all play in securing critical information.

It is our responsibility to reach out, to help others anticipate the next curve, to create this new mindset in the village. We must help others think globally and see both the forest and the trees, so together we may navigate this dangerous age. The time has come to facilitate interaction and education throughout our communities and to create a more successful environment for information systems security. The time has come to create the Information Security Village.

About the Authors

David Lam, CISSP, is the Director of Information Technology and CISO for Stephen S. Wise Temple, a K-12 school, as well as membership director for the Los Angeles ISSA Chapter. David can be reached at dlam@WiseLA.org.

Kimberly Pease, CISSP, is Vice President of Citadel Information Group, an information security management services firm and education director for the Los Angeles ISSA Chapter. She can be reached at kim@citadel-information.com.

Stan Stahl is President of the Los Angeles ISSA Chapter. His day job is President of Citadel Information Group. He can be reached at stan@citadel-information.com.

Kurt Takamine is the Chair and graduate professor for the Department of Organizational Leadership at Chapman University. You can reach Kurt at takamine@chapman.edu.

5 P. Senge, *The Fifth Discipline: The art and practice of the learning organization*, New York, Currency Doubleday (2006).