Integration

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

A reader recently sent me a request for comment about the beliefs of some of his colleagues who “insist on treating infosec as a stand-alone discipline and reject the premise that infosec falls within a continuum of security skills/disciplines and ought to be considered an organic part of the whole effort.” It seems that despite the correspondent’s and his team’s best efforts to “build a case for essentially seamless integration of infosec, both intellectually and organizationally, within the fabric of the overall security function,” higher-ups persist in keeping information security isolated as a specialized area divorced from wider strategic thinking.

First, for many organizations, information strategically important rather than simply tactically useful. That is, the ability to attain long-term objectives is profoundly affected by the security (confidentiality, control or possession, integrity, authenticity, availability and utility) of information. Information can provide competitive advantage, influence decisions on new business initiatives, determine rational allocation of resources and support effective evaluation of results. Protecting information cannot efficiently be relegated to an isolated corner of the organization; such isolation interferes with the ability to meet strategic objectives.

Second, information security is more than computer security. Most organizations keep information on paper as well as electronically; all organizations depend on the knowledge, judgement and honesty of their employees or members. Maintaining the six elements of information that we protect inevitably involves attention to physical elements of the environment, information technology and human factors. Human factors include policies, procedures and standards; hiring, management and firing; awareness, training and education; monitoring and enforcement. All of the experience of our industry teaches us that securing our intellectual capital requires a thoroughgoing change of corporate culture. Security, like quality, is a primarily concerned with process. Keeping information security out of the global consideration of risk avoidance strategies is inefficient and unwise.

Third, experience teaches that governance of security is best established through an organization-wide working group rather than by a group working in isolation. Typically, a security working group includes representatives from such areas as finance, operations, facilities, human resources, corporate counsel, information technology, public relations, and staff council or unions. We _need_ the perspective and experience of people who know what is happening in the trenches and who can speak to the operational consequences of proposed security measures. The last thing we want is a bunch of techies developing policy in a virtual reality divorced from the real-world needs of the people they are supposed to be supporting.

Fourth, two of the most critical areas of strategic risk avoidance are business continuity planning (BCP) and disaster recovery planning (DRP). Neither can succeed without thoroughgoing integration into the fabric of the organization. Neither can succeed without thoroughgoing support from the highest levels of the organization. It is simply impossible for an isolated group to establish BCP and DRP.

Fifth, facilities security personnel are essential for the success of information security. As
everyone knows (or ought to know), physical access to computer equipment allows breaches of all six of the fundamental elements of security. Facilities security personnel support identification and authentication functions; they help prevent physical attacks on infrastructure through alertness and responsiveness; they identify problems and potential problems as they conduct surveillance; they are often among the first responders in emergencies. Tight coordination between the information security team and the facilities security team makes sense.

Finally, I have always felt that the appropriate level of governance for information security is to have a Chief Information Security Officer (CISO) who reports at the same level as the other C-level executives. This structure prevents a conflict of interest that can arise when the CISO reports to the Chief Information Officer (CIO) and conforms to industry consensus about the separation of auditing or regulatory functions from the areas being monitored (e.g., there is typically a Controller as well as a Chief Financial Officer at board level; the head of financial audit does not normally report to the head of accounting; the head of operations quality control does not normally report to the head of operations).

So all in all, thoroughgoing integration of information security into the strategic planning and governance of an organization makes sense to me.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.