Security Decision Support

Decision support for security focuses predominantly today on low-level decision-making surrounding technical matters. While many enterprises use a wide variety of text-based support tools, like books, Internet sites, and email lists, to support their process, these are predominantly in the way of background information and are not informative with respect to specific decisions. Many organizations use consultants of various sorts, or outsource some aspects of their process to experts in order to get better judgment than they have internally for security-related decisions. Again, this represents an inability to make sound internal decisions about security-related matters.

Area	Policy Standards Procedures	HR Legal	Risk	Testing & Change Control	Technical Safeguards Physical / Information	Incidents	Audit	Knowledge and Awareness	Document
Create / Specify	1E-	0	3B-	0	0	0	1M+	0	0
Manage	3E	0	3B-	1E	4E-	1E-	1M+	6E-	0

The Decision Support Market Place for Strategic Decisions

While tactical decision surrounding what patch to load and whether or not to respond to an intrusion may be handled to a lesser or greater extent by technology combined with enterprise characterizations, the strategic level is largely devoid of any useful technological support tool. Management has some limited tools for policy and procedure selection, largely involving the use of automation to help write policies and apply existing standards, but these tools largely ignore the decision maker and focus on the paperwork reduction aspect of information technology. The HR, legal, testing, change control, technical safeguard, incident handling, knowledge, awareness, and documentation realm have essentially no executive support for decision-making, and this is the place where the most important decisions must be made. Tools at the management level tend to provide only limited decision support and are primarily oriented toward providing roll-up reports of lower level data.

Strategic decision support tools in the security arena that have reasonable use tend to come from analyst firms, and they are typically used as printed documents rather than as tools. While the holy grail of "Best Practices" is waived like a flag at every opportunity, when the details come out, most of the "best" are not very good and most of the "practices" are not practiced. Best practice, if there can be said to be such a thing for information security, come down to process. Process implies not only sequences of activities that are carried out, but also decision-making that is regularized and systematically applied. This is where the tools most often fall over. While it is straight forward to use a ticketing system to implement a process and assure that it is carried out, the decision making surrounding element of the process and alterations to it, while documented, remain mysterious and not well formed. The lack of tools may be the result of lack of market – or it may be the other way around. We believe it is the lack of decent tools that drives the lack of a meaningful market.