The emerging strategic risk management space

The strategic risk management space is surprisingly lacking in serious entries, especially considering the extent to which it is core to security standards and a fundamental tenant of all information protection. At some point the question of “Why?” has to be asked. In our view, the emptiness of this part of the space is due to its nature.

Risk management is, above all, a management activity, and in order to manage risks of the magnitude of information-related risks to modern enterprises, the decisions have to take place at the highest levels of enterprises. While many enterprises delegate IT risk management to CIOs or levels below them, the risks being managed are often quite literally the entire value of the enterprise. Multi-billion dollar enterprises have failed completely due to information protection failures, and yet most top management remains blissfully unaware of the realities of the risks they face. Unless and until this changes, risk management will not be properly done and the tools to support it will not penetrate very deeply into the market. That explains why risk management is bleeding edge and has poor adoption. But it doesn't explain why there are few serious contenders in the space.

Area	*Bleeding edge poorly adopted*	*Few entrants in the market*
Create / Specify	***B-***	***3***
Manage	***B-***	***3***
Process	***E-***	***3***
Execute	***E-***	***3***

The Emerging Risk Management Space

The lack of serious entrants is related to poor understanding by product developers of the issues of risk management and the lack of effective metrics in the security space. There have long been risk analysis companies that address probabilistic risk assessment and there are products that provide simple calculations and categories that can be filled in with actuarial figures if such figures can be found. But the nature of risk management in information protection is that decisions cannot be readily calculated based on formulas, the data required for such calculations is not available and when some data is available it is not very reliable, and risk management is a process that has to be undertaken, not a mechanical exercise.

Technology has a place in risk management, and that place has yet to be properly characterized or properly populated. As a result, only a few companies that seem to “get it” are in the product space. The predominant mode for risk management supplied to enterprises today is through consulting firms. These firms help enterprises develop internal process or, in some cases, perform portions of the process for their clients. To carry this process out, many such firms use internal tools and, in some cases, provide those tools to their clients. These tools generally help to gather data from people, analyze that data, and support the decision-making process. Some companies use tools from the open market to augment their services and some of the tool providers provide consulting services associated with their tools. In most cases, a combination of services and tools are used to facilitate the process.

Conflict of Interest disclosure: Fred Cohen & Associates provides risk management and related services to clients and supports those services with tool similar to those discussed.

Desirable properties of risk management software

Risk management software for information protection (as opposed to software that uses the term risk management without dealing with organizational risks or management decisions) should be focused on helping executives make decisions surrounding the acceptance, transfer, mitigation, or avoidance of business risk associated with content and its utility.

In order to be useful at this level, such software should present information on risks in a form that is meaningful to top-level decision-makers. Some consensus is gathering around the notion that metrics for executive use should be structured top down as relating to (1) business unit, (2) application or business function, and (3) business resource (sometimes called an asset). This presentation (in its various forms) appears to resonate with executives who think of their businesses in this way and provides information allowing the executive management team to act by managing those responsible for the risks.

By its nature, risk management has strategic and tactical elements. At the tactical level there is real-time management of incidents, covered under “Incidents” in our model. This is only loosely tied to the sort of strategic decision-making identified here as risk management. To the extent that executives are involved in incident handling, it represents a failure of strategic risk management. They have accepted a risk they should have avoided, mitigated, or transferred.

Interesting tool companies

The companies listed here provide commercially purchasable tools in the risk management space. This list is not comprehensive in any way. It represents companies that FCA feels provide useful and innovative tools oriented toward risk management decision support:

- **ClearPoint Metrics** (http://clearpointmetrics.com/) ClearPoint Metrics is a relatively new company that released its first product in May of 2006. The product is designed to support the creation of metrics by their customers. In essence, they provide tools to allow enterprises to collect, fuse, analyze, and present enterprise security metrics to decision-makers. As a risk management space company, they provide what amounts to a toolkit for developing and applying metrics to making risk management decisions. They don't provide details on existing threats, actuarial data, or predefined approaches to the creation and presentation of risk management data to executive management, however, their tool does provide a very nice capability to generating documentary reports that are amenable to executive review and understanding. Consultants and enterprises are likely to find that this product is easily leveraged to support their internal efforts. But the story doesn't end there. ClearPoint also provides a very nice design capability for gathering content from enterprise sources and fusing it together to provide information required for these reports. Unlike network oriented real-time security event management systems that collect a limited subset of similar content, ClearPoint is designed to take periodic data feeds and provide periodic reporting based on those feeds. It has a reasonable library of pre-defined metrics that are similar to those of other companies, but the design capability sets it apart as a tool that makes a complicated job easier by automating the things that don't require a lot of thought. It frees up the designer to design the results instead of manipulate the data.

- **Modulo Security** (http://www.modulo.com/) is the largest information security consulting firm in Latin and South America with several hundred full time consultants and internally developed tools used for thousands of enterprises over a period of years. They have leveraged their internal tools to provide “Risk Manager” and they are now partnering in the United States to provide this product and capability to enterprises in North America. RiskManager is predominantly a tool that provides clarity surrounding sources and calculations associating risk to business units, applications, and resources, in that order. It provides a variety of importing capabilities to leverage existing content from enterprise repositories such as inventory systems; allows the risk manager to associate value with resources, applications, and business units; and allows threats to be associated with these to produce relative risk levels associated with each entity covered at each level addressed. The tool provides user solicitation in the form of surveys and work flow capabilities to track those surveys as they collect relevant data which is then used in analysis. Modulo clearly recognizes the need to apply expertise to risk management and the limitations of survey tools and automated data gathering methods and moderates these with business judgment provided by its formidable consulting group. In the process of moving to the United States, its strategy is to ally with other companies already in the market, and this will, no doubt, create incompatibilities of expertise, viewpoints, and lower the quality of results, but this is simply unavoidable given the need to rely on unrepeatable processes based on judgment. Their significant libraries and support in the form of updates to threats and their capabilities is one of the key features of their product and the supporting services, and this makes then the most formidable contender in the space today.
- **RiskWatch** (http://www.riskwatch.com) is one of the best known and oldest providers in the space and they provide a platform for performing vulnerability assessment, risk analysis, and compliance reviews based on ISO 17799:2005, FFEIC guidelines, SOX, and other similar mandates. It does combinatorial modeling and has large numerical libraries covering select security events, costs, and countermeasure effects. They provide training and certification programs, assistance in assessments, and samples of completed risk assessments. RiskWatch is designed as a tool for internal risk assessment teams and requires their expertise for its utility. It uses a model (examples from their brochure) based on assets (hardware, systems, software, applications, databases) linked to losses (delays and denials, fines, disclosures, modifications, direct loss) linked to threats (disclosure, hackers, fraud, viruses, network attack) linked to vulnerabilities (acceptable use, disaster recovery, authentication, privacy) linked to controls (change control, policies, procedures). RiskWatch has real strength in its libraries that are based on data gleaned from more than 1,000 customers and internal research. These produce default values that are user alterable. Based on these values, it then does Monte-Carlo simulations of variances in threats and/or PRA and recommends mitigation strategies rated by return on investment. It gathers data via Web-based surveys or stand-alone interfaces and includes hosted services if desired.

While there are a lot of other products in this space, these represent the core elements of the available approaches and help to understand the market space as it exists today. These vendors were also rated as honest in the claims provided for this assessment based on discussions of those claims and evaluation by our internal experts.

