Emerging Market Presence

The emergent market presence chart indicates how many small companies are in each area of the market space. The table is followed by a brief analysis of the emerging market. The advantage of the emerging market view is that it shows where niches are and are not as well as the progress in the market toward meeting overall coverage of the security space.

Area	*Policy Standards Procedures*	*HR Legal*	*Risk*	*Testing & Change Control*	*Technical Safeguards Physical / Information*	*Incidents*	*Audit*	*Knowledge and Awareness*	*Document*
Create / Specify	*1*	*0*	*3*	*0*	*0*	*0*	*1*	*0*	*0*
Manage	*3*	*0*	*3*	*1*	*4*	*1*	*1*	*6*	*0*
Process	*6*	*0*	*3*	*4*	*20*	*8*	*3*	*8*	*0*
Execute	*5*	*1*	*3*	*10*	*125*	*39*	*5*	*11*	*0*

How many companies and where they are in the space

The counts in this chart are based on representations made by vendors as reviewed by FCA. No effort was made to test products or review them with users to verify their location in the market space, their viability, or other information about them. The survey is skewed toward technology companies with products, however we believe it represents the larger market.

Analysis

Clearly the market remains very execution oriented with some small drive toward process but little effort being put into the management or executive level decision-making process. While risk management, education, policy, and awareness are starting to emerge from the technical space toward the business and process areas, this emergence is slow. The low counts in audit represent the fact that audit is relatively mature rather than that it is lacking, while low counts in Documentation, HR, and Legal areas indicate a lack of technology to support these areas of the market. Change Control is a key early stage area that could break out in the coming years, largely driven by regulatory drivers and the need to get better control over IT assets and provide increased information assurance as risk is better understood.

A very large and unsettled area of the market is in adapting to the Network Admission Control push of Cisco. Many vendors are working to provide solutions in this space, predominantly to manage these mechanisms and to integrate them with end point technologies and alternative routing and switching infrastructure. Endpoint solutions are integrating access controls to limit the use of removable media, to mix health checks of NAC with configuration management, and to a lesser extent, for patch management. Accounting for software presence and limiting execution are becoming common as is linkage with identity management and provisioning.

Copyright(c) Fred Cohen & Associates, 2007 - All Rights Reserved

Network firewall appliances with content control, NAC, and SSL VPNs are an increasingly crowded space in the market, driven by high price points, low cost hardware, and chip level content inspection. Many products in this space license elements of the technology from other providers and perform integration to produce the mis-named “unified threat management” systems that are not unified, don't manage, and deal with attacks, not threats. In market speak, this rolls off the tongue and puts visions of joy in the minds of customers, so the obfuscation continues. Some are pushing into the SMB market with relatively low-cost solutions. Service providers do pattern updates to create a service market that also drives down acquisition cost. Linkage to identity management is increasingly embedded to allow centralized control of gateways and end points. Convergence of these areas is clearly in the cards. Margins for companies like Cisco are destined to fall as the chip providers and appliance vendors emerge with compatible sets of devices and controls that cover all of the existing Cisco and other switching and routing infrastructure elements. A shake-out is inevitable and may start within a year.

A few interesting niches are noteworthy. The Trusted Computing Group standard has reached a very substantial portion of the hardware in the world and is starting to be interfaced to software and operating environments. This will produce a dramatic improvement in end points and infrastructure integrity. The deception niche now has several participants and limited acceptance in the DoD and SMB niches. It is largely based on honey pot technology and invisible routers, that automatically respond on addresses and ports to disrupt scans. They lack linkage to identity and network management systems, making management complex, but as acceptance grows, this will change. The education niche is growing as more universities embrace information security as a continuing education area and start to grant masters degrees. With very few exceptions, they are still at least 5-10 years from recognizing security as an engineering discipline, but MBA programs are starting to add concentrations in this area. In the risk management arena, several companies are making a push toward providing information on overall business IT risk to managers and executives, something not been done by the many products claiming to be in the risk management space for many years. Code quality companies are emerging to fill the technical aspects of testing, application gateways continue to bloom, and outbound content inspection to prevent leaks is growing.

A few wild cards are also in the market. Flash video cartoons for security awareness is being introduced while search engines are being fused with log collection to enhance examination of log and surveillance data. Change management is being automated with lock downs of end points and work flow process to limit authorized changes to authorized times under proper approvals. Code obfuscation to limit reverse engineering continues to persist despite 30 years of lackluster performance.

Increasingly, even the newest entrants into the market have a broad range of coverage. While narrow niches continue to exist for select areas and some new ideas stand on their own, the market is driving toward combined solutions and integration across a broader range of areas in order to deal with enterprise-level solutions. Consumer-level products are rarely able to handle enterprise needs, and even medium sized businesses are being served with complex arrays of features involving a wide variety of controls. The complexity of management is increasing but there remains little progress in the way of tools to manage that complexity.

Copyright(c) Fred Cohen & Associates, 2007 - All Rights Reserved