Market Roundup

December 2, 2005

Microsoft Partners Offered Revamped Security Competency

By *Joyce Tompsett Becknell*

This week Microsoft announced a restructured Security Solutions Competency for its Partner Program in partnership with long-established certification programs from International Information Systems Security Certification Consortium (ISC)² and Information Systems Audit and Control Association (ISACA). According to Microsoft, the redesigned competency now includes two new specializations, one focused on security management — designed for partners that focus on services such as security policy, governance, compliance, risk assessment, risk management, and auditing — and another focused on infrastructure security, dedicated to the technical, Microsoft-product side of security. As part of Microsoft's ongoing commitment to making the Windows environment more secure, the program was changed to make it more useful to partners who work with products, solutions, and services that are based around security. Microsoft also believes that this will lead to enhanced revenue opportunities to partners who take advantage of the certification to grow their security expertise. Microsoft says it has made investments in changing the Security Competency and providing field resources to support its security partner ecosystem, and that it will continue to do so. According to Microsoft, the Microsoft Partner Program will work with security professionals to validate their certifications through (ISC)² and ISACA, and when partners register as Microsoft certified security partners, their certifications will be validated through the two organizations.

Microsoft has dedicated itself to making a more secure mousetrap for quite awhile now. A large part of that dedication has focused first on Microsoft products, taking care of weaknesses or potentially exploitable features, and creating a formal program for making updates more manageable. But that is only one part of the problem. There's a bigger problem with the environment itself. Some parts of the IT environment are better protected than others, and when IT managers first started using Microsoft products the network did not extend quite so far into the ether(net) as it does now. The original IT environment for most companies probably didn't' require as much security as more of the network was isolated. That means that IT as an industry is still learning how to impregnate security in everything it does as a mentality and discipline, and as a set of practices rather than as a set of products. With this in mind, we believe Microsoft is taking the right approach to security by making sure their vendors understand not only the secure way to approach Microsoft products, but also the secure way to approach IT. Microsoft customers may not see this commitment in their everyday dealings with Microsoft and its products, and we believe it is important to point this out.

Security for an IT infrastructure is the responsibility of everyone, including IT managers, individual users, and business executives. Companies depend on vendors to provide them with the most secure products possible, but they also need partners that understand security when they get involved. Business partners should take advantage of this certification, especially as it extends to technology-agnostic areas and provides skills transferable beyond the Microsoft products to the rest of the IT infrastructure. We agree with Microsoft that astute business partners should be able to leverage this knowledge into greater revenue opportunities and an ability to differentiate

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

sageza.com

themselves, as security is never going to become less important to any organization, and is becoming crucial to a growing number of organizations regardless of what applications they run or what industry they are part of.

ELF Debates

By Susan Dietz

At the annual European Leadership Forum (ELF) meeting in London on Tuesday, the protection of intellectual property rights (IPR) featured prominently. Larger software companies' representatives, such as Microsoft's EMEA president, voiced their concerns over the protections of IPR, especially in China. Smaller companies, most notably led by Skype's CEO, argued that too many software patents stifled innovation. Even service providers piped up with BT's CTO Matt Bross landing in the middle of the debate, predicting that within a few years — when China has generated more of its own intellectual property — then the IPR of other companies will be protected much more diligently.

This latest salvo in the IPR wars shows more players jumping into the fray, and while it will probably not bring about all sides agreeing on every aspect 100% of the time, it will perhaps lead to an eventual armistice. It's said that a good compromise is one in which all parties are equally unhappy; and we can see glimpses of that happening here. When China finally chimes in with its own demands for the respect of IP, we believe the weight of opinion will force the smaller companies to accept that they must start playing the patent game more vigorously. On the other hand, the current practice the larger companies have of applying for hundreds of patents is clogging the patent offices and will most likely need to be seriously curtailed.

Over-zealous patent applications may stifle creativity and innovation a bit, but when a company develops a truly new technology, there will be a niche in the marketplace for that company and its products. There are rumblings in Washington about overhauling the patent process anyway, at least in the U.S.. If smaller companies want to ensure a more open environment for developing software, now is the time for them to make their voices heard, and not just in the IT community. Politicos in Washington and other world capitals need to be made aware of any inequalities in the system before they can fix those same inequalities. That may sound a bit naïve, but sometimes the system does actually work. Let's hope that's the case in this instance.

Ongoing OneCare? Microsoft Opens to Public Beta Test

By Clay Ryder

Microsoft has opened up its impending OneCare Live security subscription product beta test to the general public. The beta software is now available free of charge from http://ideas.live.com for testing by anyone with a U.S. English version of Windows XP SP2. OneCare is targeted at consumers and includes anti-spyware, antivirus, firewall, and several configuration tune-up tools for Windows PCs. The antivirus capability is expected to be based upon the technology Microsoft acquired when it purchased GeCad Software at the end of 2004. Microsoft has not announced pricing for OneCare but has said the offering will be a subscription service that will become available in 2006.

This announcement and its predecessors are interesting from a technological standpoint, but perhaps more so from a pricing model perspective. While Microsoft has engaged in site licensing with larger customers for years, the notion of ongoing licensing payments in exchange for current versions of software is something that Redmond Giant rarely, if ever, has undertaken in the consumer marketplace. Outside the upper echelon of corporate grandeur, most businesses and consumers have simply bought their software through a business partner, catalog, or local electronics geek shop. This approach generates a one-time expense; however, the customers tend to purchase upgrades on their own timeframe which generally does not coincide with scheduled product releases from vendors. Also, some would tend to buy their software on a purchase-once-use-many basis for their various machines. In a physical product delivery scheme, this is hard to control. However, a subscription model based upon Internet connectivity changes the game considerably where software can be locked to a certain hardware signature.

Software vendors have been under pressure by the open source movement, and by changing expectations in the marketplace, regarding the value proposition of software in general. Open Source, or free, software is enigmatic to a vendor that derives the bulk of its revenue from shrink-wrapped software sales. However, the same software when delivered in an alternative pricing structure may find itself welcome again, especially if the perceived price is lower. Enter the subscription or leasing model. To us, Microsoft's embracing this approach to a software solution that will require continuous updating to be most effective is a clever move. The value delivered in prophylactic software is actually more about future nefarious encounters than the virus, malware, and security exploits that already exist. Once a system is cleaned and protected against the known, the focus shifts to the unknown, which by definition is not part of the software when installed. Thus, the ongoing updates to virus definitions et al are a key part of such a solution. The research and protection against such malevolent cohorts is an ongoing value, and one that is delivered on an ongoing basis. Thus, pricing in this fashion closely matches the value delivered with revenue generated. Although the consumer market readily accepts subscription services in other markets such as telephony, cable, video rental, car leases, etc., in software it may take some cultivation. But this is one of the strengths of Microsoft: oodles of money with which to market. So while it may take some time, we will be watching in the wings to see if the Redmond Giant is successful in changing a basic behavior in the consumer software marketplace to embrace a subscription approach to system level software. If successful, we may witness a further movement towards software as a service, as opposed to a product.

EU Civil Liberties Meets Data Retention Redux

By Joyce Tompsett Becknell

This week, the civil liberties committee of the European Parliament voted in favor of the directive on data retention, which would require communications service providers to keep details on telephone calls and Internet use (not including content) for six months to a year. The directive seeks to standardize the amount, type, and length of time SPs must store details, including fixed-line call details of caller name and address, number dialed, and receiver name and address, as well as call start and end time. Mobile phone information would include subscriber SIM or identity and location, and Internet data would include computer IP address, telephone number, subscriber name and address, and login/logoff time. The data held would not include the contents of the communications, but instead would allow law enforcement agencies to identify sender and recipient, and with mobile calls, location. The full parliament will vote in December on the rules which if passed must then be approved by individual member states.

The idea of this law raises issues in two spheres: the technical and the personal. On the technical side, the directive raises several issues. First and foremost is the notion of the cost to service providers. The committee did vote that member states should reimburse telecommunications firms for the additional costs of complying with the rules. This may be some small consolation. Or maybe not. Beyond the initial costs of adding infrastructure, there are issues of ongoing costs, limitations on data types, and problems with the length of retention periods. European telephony, mobile phone, and Internet companies have declared the retention periods too long and the scope of data too wide. In essence, telecom companies have it easiest as they already track most of this information with normal billing. With the exception of location, mobile phone companies are almost there. But Internet companies, especially those dealing with broadband customers, may have a harder time. As usually happens with these things, the idea sounds really good but the practice quickly proves to be much more difficult. In the U.S., the Sedona Conference is a group of jurists, lawyers, experts, academics, and other interested parties who have developed an ongoing dialogue to sort out issues including topics such as managing information and records in the electronic era in order to advance U.S. law. One EU directive that spans the entire communications industry with a broad brush seems overly ambitious in comparison. And some states had wanted even longer time horizons and more data than that which the committee approved.

On the other side, of course, are the personal issues of privacy and rights. A number of human rights and civil liberties organizations have taken issue with the original directive. The committee did insert a provision to ensure "effective, proportionate, and dissuasive penalties" for infringement of the rules. It also decided that only a judge could authorize access to telephone and Internet traffic, which wasn't specified in the original version. Again it sounds like a good concept in theory — getting information to law enforcement to combat crime and terrorism — but getting that information, maintaining it, and protecting it are much more difficult to do as the volume scales. We're confident that this will be sorted, but we're pretty sure the road to get there is going to be long and bumpy.