VERITAS SOFTWARE CORP /DE/
Form 425
February 08, 2005

Filed by Symantec Corporation Pursuant to Rule 425
Under the Securities Act of 1933
And Deemed Filed Pursuant to Rule 14a-12
Under the Securities Exchange Act of 1934
Subject Company: VERITAS Software Corporation
Commission File No.: 000-26247

This transcript contains forward-looking statements, including post-closing integration of the businesses and product lines of Symantec and VERITAS, forecasts of market growth, future revenue, benefits of the proposed merger, and expectations that the merger will be accretive to Symantec s results and other matters that involve known and unknown risks, uncertainties and other factors that may cause actual results, levels of activity, performance or achievements to differ materially from results expressed or implied by this transcript. Such risk factors include, among others: difficulties encountered in integrating merged businesses; uncertainties as to the timing of the merger; approval of the transaction by the stockholders of the companies; the satisfaction of closing conditions to the transaction, including the receipt of regulatory approvals; whether certain market segments grow as anticipated; the competitive environment in the software industry and competitive responses to the proposed merger; and whether the companies can successfully develop new products and the degree to which these gain market acceptance.

Actual results may differ materially from those contained in the forward-looking statements in this transcript. Additional information concerning these and other risk factors is contained in the Risk Factors sections of Symantec s and VERITAS most recently filed Forms 10-K and 10-Q. Symantec and VERITAS undertake no obligation and do not intend to update these forward-looking statements to reflect events or expectations regarding the circumstances occurring after the date of this transcript.

The following is a transcript of the keynote presentation given by John W. Thompson, Chairman and Chief Executive Officer of Symantec Corporation, at the Thomas Weisel Tech 2005 Conference on February 7, 2005.

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference
Event Date/Time: Feb. 07. 2005 / 3:15PM ET streetevents@thomson.com 617.603.7900

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference CORPORATE PARTICIPANTS John Thompson *Symantec CEO* CONFERENCE CALL PARTICIPANTS Tim Klasell *Thomas Weisel Analyst* PRESENTATION John Thompson - *Symantec CEO* Intent to merge with VERITAS strengthens our story, not just in the backup and recovery space for which VERITAS is so well known for, but for its focus on provisioning and managing systems in the heterogeneous environment that many large enterprises have. Before I get into the story, let me remind everyone that there are forward-looking statements that will be made here and so you should be mindful of that, as you consider our Company. Furthermore, here very shortly because we are involved in a public company transaction, we will file a proxy statement that we would like for all of our investors to review so they understand the specifics of the transactions and can pose any questions that they might have of us, based upon that document. Now let me put in context what we think are the important trends in our industry and why we re doing what we re doing. This is in fact grounded in our belief that started to emerge in mid to late 2003. They were trends that we not only saw ourselves, but also were spotted by Booz Allen, which is a firm that we tend to track their view of the industry quite closely. First, large enterprise buyers in many respects are interested in reducing the complexity associated with managing their infrastructure. In other words, all of the software products that they buy on which applications are then run, they would love to have that done in a less complex way. Furthermore, they would like to do that with fewer vendors. It is not uncommon for large global company to have literally hundreds, if not thousands, of IP suppliers for both software and services around the world, and therefore if they can aggregate more of their buying with one company that would certainly streamline some of their own internal processes, not just getting at the complexity of the products themselves. Second, in all software businesses around the world, particularly in the security and infrastructure market, the shortage of talent to be able to deliver or install the products that are being acquired is becoming acute. Therefore, services is a very important complementary component of the software business itself where customers will avail themselves not just of the software capability that the company has, but also the services than can be wrapped around the software. Next, it is clear that wireless will be an issue that we will all have to deal with but I would posture with you that the issue is not solely about securing the wireless experience, which is something we are clearly focused on, but for large enterprises it is also about managing the wireless environment. In other words, understanding where the devices are, what applications they have excess to, what the current state of the device is, and how in fact they can control the availability of information that is flowing to and from that wireless infrastructure. So while security is important, the management of the infrastructure, the wireless infrastructure is as important. Fourth, it is clear that Linux has arrived and has arrived with a vengeance. Few large enterprises today have only Windows or only a UNIX environment. Most of them for specific application purposes have in fact deployed Linux solutions. So the one thing that Linux does assures us that the environment that large enterprises are dealing in will be heterogeneous. In other words, there is one more platform that we as software companies, we as service providers, are going to have to support. And the issue for Linux is not just how well does it do at the server level, but how quickly might it spread to the desktop level specifically for purpose-built applications within a large enterprise environment. It is our belief that a heterogeneous software company managing the multiplicity of platforms that customers have deployed is a strategic advantage for us and for our customers, hence that is pretty much why we are doing what we re doing. Finally, given the amount of activity going on in the marketplace where software companies need to scale up to address the global needs of their customers, and given the need for a more complete solution set or complete portfolio, it is apparent to us that the needs to merge for the consolidation activity will continue in this industry, and to the extent that we are positioned to be consolidator, obviously the actions that we have taken would suggest that we are not at all bashful about participating in that way. Now, in February of last year, about a year from now, we introduced the concept of convergence which was where streetevents@thomson.com 617.603.7900 www.streetevents.com 1

network management, systems management and storage management are all coming together. At the center point of this convergence is the desire by customers to insure not just the availability of the information or the security of the information, but to insure its integrity. We have an unparalleled understanding of what the threat environment looks like because of the sensor network that we have deployed around the world that literally tracks every virus, every attack, 600 to 800 customers around the world in literally thousands and thousands of networks. So the question is can you take that intelligence that you have about what is going on in the Internet environment and translate that into operational tools that will protect data or provision systems more acutely or quickly. We believe that this notion of automated provisioning will complement what we do in the security protection space, because it will allow you to reconfigure a server or push a software patch or rebalance the workload on a server farm to insure the availability of the critical data that many large enterprises are using to run their businesses today. So it is this view that leads us to the belief that we have to do more than just be in the security business, that we have to do things that are complementary to the security business all-around provisioning the Windows, Linux, and UNIX environments for large enterprises from the desktop to the largest server farms that might be out there. We think those trends suggest that individuals and enterprises are absolutely exploding with digital assets. Today, even individual consumers have an enormously growing portfolio of digital assets, be it their photographs or their MP3 music, or whatever it might be, and all of that not only must be protected, but in many instances it needs to be backed up and archived such that it can be retrieved at some point in time. That is very true for large enterprises, particularly in an environment where compliance is also a relevant issue. So being able to not only know what you have, but to be able to retrieve it consistent with the regulatory initiatives that may be affecting your company are really, really important. It is clear that these environments are heterogeneous and they will stay that way. While our friends in Redmond might like to think that the world is all Windows, the world is not. The world is permanently heterogeneous and that is advantageous for an independent software company that delivers market leading capability on all platforms. Clearly customers have a cost mentality today and much of what has gone on is focused on cutting costs in the labor arena. Because the hardware costs have come down quite substantially over the last few years, software costs while they have been growing, the growth in labor cost has been far, far outstripped that of hardware or software. So their focus is, how can I deploy a software layer that helps me manage both the complexity and costs associated with delivering a compliant resilient environment. We believe in the security domain that the frequency and complexity of the threats that we re seeing will continue. Today, it is unthinkable that someone would be unprotected as an individual consumer on a broadband connection. It is also unthinkable to think that a large enterprise would not use proactive technologies to protect themselves from today s threats. The vulnerability window 18 months ago used to be on average, 6 to 9 months. Last year, in the last half of the year, the average vulnerability time between discovery and exploitation shrunk to less than 6 days. So what that says is customers have very little time with which to react to the announcement of a new vulnerability that has been discovered and putting in place the right protection or availability strategies to protect their infrastructure. Let me give you just a brief example of that problem. In early 2003, there was an attack on th e network called Slammer. Slammer occurred in the January/February time frame of 03. And from the moment that the vulnerability was discovered to the moment that the exploit was released, would literally 6 months and customers had 6 months to plan for where are the vulnerable systems that might be affected by this particular vulnerability in the Windows environment. And low and behold, even with 6 months notice, customers did very little. As a matter-of-fact within a matter of hours after the release of the exploit for that particular vulnerability, the rate of infection was doubling every 8.5 seconds. So we reached the point within 2 hours from the initial attack that hundreds of thousands of systems were rendered inoperable, ATM networks, airline traffic control systems. A range of mission

critical systems were affected to the point where availability of data and service to customers was significantly disrupted. Now all of the security protection technologies in the world did not stop Slammer. As a matter-of-fact, it required a combination of technologies to be affected, hence the concept that we have believed for quite some time and were streetevents@thomson.com 617.603.7900 www.streetevents.com 2

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

the innovator of, which is integrated security, implied that you need multiple security technologies at multiple tiers of the network in order to be effective in dealing with these kinds of threats. However, in this particular case, had customers known what systems were affected, known what the state of those systems was, in afterwards what software is running on those systems, and had a sense of how they could distribute a patch, they could have mitigated much of the risk of damage associated with this particular attack. This was when they had 6 months notice. Shrink that to less than 6 days, and what it suggests to us is automation and the whole notion of insuring availability and integrity is more about a management process than a security process alone. Hence, that is why we believe the transaction with VERITAS is so important to our Company. What we bring together is the leading security management company with the leading availability solutions company to focus on a concept that we launched last fall long before this transaction called information integrity. Which is how do you help customers keep their systems up and running no matter what happens. We believe by focusing on availability and the ability to secure information, you end up with a more complete solution that allows the customer to think about the 3 fundamental tenants of what is going on in their environment. Understand what is going on, act on that insight, and insure that I have the proper or adequate controls in place. If you look at the portfolios of the 2 companies, they are very, very parallel in the sense that there is minimal overlap. We lead in the security space, VERITAS leads in the storage and systems management space with some areas of overlap, particularly, where we are in the services business or in overlapping the Windows platform where we had been a very strong player and VERITAS had capability there as well. So what this says is that rather than our engineers spending all of their waking hours over the next few months trying to rationalize the product portfolio in whose technology will win over someone else s in the same company, they will be focused more on the market opportunity for expanding the capability for our 2 companies. There are 3 areas where we think there are wonderful opportunities right out of the shoot. The first is what we call the resilient infrastructure which is about how do you automate more of the processes for reprovisioning desktop and server devices based upon knowledge and insight that you have about potential vulnerabilities in network reaches. The second is around the e-mail environment, the mission critical application for many large enterprises today is mail. And so how do you insure not just the integrity of the information that is coming through the mail system, but how you archive it and retrieve it to conform to the changing regulatory environment for many industries. Third, regulatory compliance. While all of us have had to deal with Sarbanes-Oxley as a horizontal layer of regulations, many industries have to deal with the vertical nature of that regulatory environment as well. It is taking the combined capabilities of Symantec and Veritas for their compliance based technologies and delivering something uniquely different into the marketplace. So diaphragmatically, take me take you through a couple of these very quickly. If we could in fact notify our customers today of a vulnerability, and today we happen to maintain the largest repository of vulnerabilities in the world through a system called Bug Trap (ph). Once a vulnerability is discovered, if we can take our understanding of that, share it with customers and have them act in one of two ways, either push a software patch to the extent they know where the software assets are that are affected, or reconfigure a device in such a way, be it a firewall or a server, reconfigure that device in such a way that it is not vulnerabl e any longer. That shear linkage could in fact insure greater availability of the infrastructure itself. If in fact we knew that a threat was ravaging its through the Internet, hence an attack was underway, we could immediately initiate a backup action. And rather than having backups based on a daily agenda or weekly agenda, you could do a real-time backup then, hence making the restoration process a lot quicker because you had more recent information that you used for the backup itself. That whole process of using intelligence to drive proactive protection and systems provisioning is what this concept of a resilient infrastructure is all about, and we believe that will help customers keep their systems up and running at a time when availability is more important quite

frankly than almost anything else. In the e-mail world, today with our antivirus technology being essentially the market leader, and with the spam detection and traffic shaping capabilities that we have, we clearly have our pulse on the mail environment around the world. More than 25 percent of the e-mail traffic in the world flows through the Brightmail infrastructure. More than 60 percent of the mail traffic today is considered to be spam. So we have great insight on what spam activity has gone on, and terrific streetevents@thomson.com 617.603.7900 www.streetevents.com 3

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

insight from over 100 million customers around the world sending us information about viruses and worms. Using that insight to ensure that we can appropriately catalog and categorize mail for eventually storing it and retrieving it consistent with the compliance environments particularly in industries like financial services, that represents an enormous opportunity right out of the shoot for these two companies. So you bring together Symantec s security scanning capability with the KVS archiving and retrieval capability that VERITAS has, and you have a wonderful marriage just to address a mission critical application called mail. Finally, in the regulatory compliance arena, clearly this environment has seen rapid change. And systems like ESM, our Enterprise Security Management system, has been abducted to deal with not just the vertical regulations assisted with a particular industry, but the horizontal regulatory environment as well, dictated by Sarbanes-Oxley. One of the things that this regulatory environment does suggest is that CIOs or IT organizations, have to have a better understanding of what is the state or status of their asset portfolio, not just the hardware devices that are there, but the software implementation as well. If you can in fact use that knowledge to manage that environment more consistent with corporate policy, IT in the future won t be the long pull for Sarbanes-Oxley 404 certification. And in almost every public company that I am aware of, where they have had to meet the regulatory challenge in the December or fourth quarter of the year, the long pull to compliance was in fact IT. So you re going to see more IT infrastructure software companies participate or focus on this opportunity and these two companies when they come together bring leading assets for the compliance environment. We have very complementary sales and coverage models where today Symantec has about 16 or 1,700 direct salespeople; VERITAS has about 22 to 2,300 covering the largest accounts. We both view it as a channel infrastructure for reaching the middle market. Ours may be a bit more sophisticated and more well established than VERITAS. There hence, might be leverage for both of us as we blend our enterprise coverage miles at the top and leverage the channel infrastructure at the bottom. Interestingly enough, we had planned and still do plan to deliver a consumer backup and archival solution this year. We now have a broader portfolio capability from which to pick and choose as to what functions we take into the consumer and small-business market. But these sales teams are quite excited. I have had an opportunity over the course of the last 3 weeks to visit both EMEA, North America, as well as Japan and Asia-Pacific VERITAS sales teams in their kickoff meetings. And almost to a person they are pretty jazzed about the prospects of having (technical difficulty) portfolio to take to their customers. If you were to look at who has said what, our customers and partners have probably had the most resounding impact on this transaction. Our partners in particular see this as a wonderful opportunity for them to expand their portfolio of offerings and our customers view this as an opportunity to interact with one vendor as opposed to many, to get a broader range of capabilities for addressing their infrastructure resiliency challenges. We have had a number of discussions and as we continue the process of talking about this with large enterprises, we will add to the list of referenceable accounts who are willing to stand up and be heard. Let me talk about the timeline for the transaction. We announced the transaction on December 16th. Others announced it a little bit ahead of that. When we announced the transaction, what we said was it is our intent to blend the leadership teams and therefore we will combine the leaders from Symantec with in fact leaders from VERITAS, to create a new company. Tha t new company will have a 10 member board it will be made up of 6 members from Symantec and 4 members from VERITAS. In January of this year right after the new year, we contracted with PricewaterhouseCoopers to work on the back office infrastructure, and Bain & Company to help us with the go-to-market integration strategy side. We just a few weeks ago cleared the Hart-Scott-Rodino review and so we are now in full mode of integration. The first set of integration meetings, formal integration meetings were launched about 2 weeks ago. It is our expectation that on or about the 15th of February, somewhere in that general time frame, we will announce the first organizational structure for the new Company. In other words, one of

the operating units, hence HR or legal or whatever, that announcement will occur. At that point, it will start the clock where over the course of the next 30 days, we will roll out organization after organization with the final one, at least at this point we believe, being the sales organization that will be announced sometime around the 15th of March. streetevents@thomson.com 617.603.7900 www.streetevents.com 4

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

We would clearly expect to have strong quarters consistent with our guided results or guided outlook for the March quarter. Sometime in the late May I m sorry late April, early May timeframe, we would hope to close this transaction. Right now, it looks more like May than April but that is just a function of getting through the process with the SEC. And the filing will occur here very, very shortly. If you were to look at this Company now over the last 12 months, what you would see is about $2.4 billion in revenue generated by the two companies, about 84.5 to 85 points of gross profit. It s got an operating margin, that when blended, will be at about 28 percent and it generates one heck of a lot of net income. In other words, this is a very, very powerful company in terms of its sheer financial metrics. If you look at its cash position, we generated between us another half of a billion dollars in the December quarter, so now the combined balance sheet would be at about $5.5 billion. The deferred revenue pool is very strong with Symantec having incredible visibility and VERITAS visibility growing every quarter. On the headcount basis VERITAS is larger than Symantec because they have chosen to outsource I m sorry offshore when we have chosen to outsource. So they offshore a fair amount of support and engineering to India and we have chosen to outsource that as opposed to offshoring that. Hence that accounts for the disparity if you will, in the headcount results or headcount position of the two companies. If you were to look at the revenue mix it will be about two-thirds to three-quarters enterprise, the balance of it in consumer. If you were to go back to what Symantec has been trying to do since April of 1999 when I arrived here, it was to transform the book of business hence the revenue flows of the Company to mirror the industry. In today s technology world, about two-thirds to three-quarters of all IT spending is done by corporate and government users. And when we combine these 2 companies our revenue flows will look more like the market, hence it positions us to be able to deal with the way the market grows as opposed to individual vagaries that might exist for a given company. From a geography point of view, the United States will represent about half the business and the rest of the world representing the other half. If ever I were to put challenges on this team it would be to have Asia-Pacific and EMEA continue to grow at a rate faster than the United States where ultimately the point of arrival is probably about 55 percent non-U.S. revenues, 45 percent from the U.S. That is a longer-term view as opposed to where we will be as we start out. What we have said is assuming the transaction closes in early April and that was the basis of our original guidance, that we expect revenues to be about $5 billion for this combined Company. We would expect to have a OpEx of about 55 percent of revenue and of that baked into our EPS forecast is about $100 million in synergies. The non-GAAP EPS forecast, again off of the $5 billion in revenue, is 99 cents which in fact would be accretive to the consensus First Call view that existed back in the December time frame when we were pulling this together. So why are we doing this? We think this addresses profound needs that large enterprise buyers have in the number one and number two spending areas that large enterprise buyers will invest in and that is security and storage management. It significantly broadens Symantec s portfolio to cover more of the heterogeneous platforms that customers deploy today. It combines two market leading companies. And so unlike other transactions where big companies buys a small company or two small companies come together, these are two market leaders coming together with significant scale and scope in their business focused on addressing a very, very important challenge for large enterprises. The addressable market for our Company will be $56 billion by 2007. As I reflect on Symantec s performance over the last 6 years, when I arrived here our addressable market was $3 billion. So the whole idea of our strategy over the last 6 years has been expand the scope of what we can address from a revenue opportunity point of view and we will get our fair share. And hence expanding the addressable market for Symantec this time around, we re convinced is the right thing. We have very, very complementary sales capabilities with 2,200 from VERITAS and another 16 to 1,700 from Symantec clearly focused on how do we not just preserve the relationships that we have with large enterprise buyers, but how do we in fact enhance and deepen the relationship that we have. Finally, few enterprise

software companies have the financial scale and scope and stability of this new Company. We are proud of what we think the possibilities are. We are just anxious to get on with the execution. Let me stop there and ask Tim to come back up and we will entertain questions. streetevents@thomson.com 617.603.7900 www.streetevents.com 5

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

QUESTIONS AND ANSWERS Tim Klasell - *Thomas Weisel Analyst* Okay, I get to ask the first couple questions because I have the mike and then I will open it up to the floor for questions. John, you ve got 5.5 billion in cash, going to fix fairly soon. You made some comments about the large companies sort of consolidating the space. If that is the case shouldn t we expect to see more, maybe not quite to the same magnitude, but the VERITAS type acquisitions rather than the last few years you ve been seeing things like Brightmail and Riptech, and of course a few others, or it s been sort of smaller technology acquisitions to fill into your productline. John Thompson - *Symantec CEO* Let s be clear about how we re going to use this case. Right now we are just going to count it. We have no intent to do anything other than focus on the integration of VERITAS. While there are any number of people in both companies that have ideas of things that they would like to go do, those are a distant thought for the moment because we have got an integration task that we much must complete. That being said, companies have been acquisitive and they have been cash acquirers. And so you should expect that as Symantec gets comfortable with the integration process here, we will bring our heads up and we will look at where cash acquisition opportunities might be. Furthermore, both companies have been active repurchasers of their shares. Symantec s had a 10b-51 program in place for quite some time now. VERITAS in the last year repurchased about $250 million worth of their shares, and so that might be a part of the capital use strategy that the new Board of Symantec would have to evaluate. But it is clear that those are the two most effective ways that we might in fact deliver value for that cash back to investors. Tim Klasell - *Thomas Weisel Analyst* Staying on the acquisition, what are the most important things you are focused in on the integration? And maybe you could give us some of the I think I asked you at the table who are the most important people you have to keep, besides Gary obviously, to make this successful? John Thompson - *Symantec CEO* Clearly it is not lost on us how we think this community will evaluate this deal, and that is how did you perform against your guidance or expectations that you set for us. That is revenue and EPS. So the only way you get EPS is to generate revenue. The only way you generate revenue is if you have a salesforce that is focused and understands not just the product portfolio but what territory they have and how they re going to be compensated and rewarded and on and on and on. So right now, the preponderance of my focus is on, okay how do we get that done? So Gary, who will run the go to market side, along with Art Maden (ph) and Tom Kendra, the two sales leaders, are working now to plan the salesforce integration and we will create one salesforce, not run with two salesforces. That being said, there are a range of people that are important in the Company, not just Gary, but all of the senior leaders because with that comes the knowledge of who VERITAS is about its products, about its customers and about its operations. And so we have structured a transaction that we think incents all of the senior leadership team to stay. So there are retention bonuses in place, there are equity awards that will be a part of that process and we are hopeful that as we look through integration, as people see meaningful jobs and meaningful opportunity, they will want to stay with this new Company. I cannot imagine a company that would be more exciting to work for, quite frankly, than this one. Tim Klasell - *Thomas Weisel Analyst* Very good. Questions from the audience? Unidentified Audience Member (Inaudible question microphone inaccessible) John Thompson - *Symantec CEO* I think the only person who can make you feel comfortable I m sorry. Tim Klasell - *Thomas Weisel Analyst* I m going to have to repeat the question for our Web audience. The question is, help those get more comfortable streetevents@thomson.com 617.603.7900 www.streetevents.com 6

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

with Microsoft and maybe give us a feeling for what you think when they announce at the RSA conference next week? John Thompson - *Symantec CEO* No one would like to have Microsoft announce what they are going to do more than us. It is very challenging to compete against the ghost. What we have been competing against so far has been the Microsoft press machine as opposed to the reality of a product. So I am hopeful that Bill or someone at RSA next week, does announce what they re going to do because then that will give you a way to gauge whether or not we are competitive and focused in the right way. That being said, our strategy has been focused on three fundamental components. One, build a feature-rich product that is easy for customers to use and buy, or buy and use. Hence all of the focus around migrating our AV base to Norton Internet Security has been a critical part of that strategy to strengthen our relationships with the OEM channel to the point where they would prefer to do business with us as opposed to anyone else. We think the strategies that we have had in place there for some time certainly they don t make us completely resilient to an attack by Microsoft but they certainly make it more difficult I think for Microsoft to break in there. Finally, don t give up any real estate. Make sure that what I mean by that is if the shelf space in the store and if the shelf space on the PC as it is shipped from the OEM is the important piece of real estate, don t give any of it up. So at the consumer level we have had a SKU strategy to put more products on the shelves and hence you ll see expanded product capability come from us later this year. And at the OEM level, we have done things to make the process of managing the security and update mechanisms of your personal PC much more painless from us than from Microsoft itself. We replaced the Window security center with the Norton security center and most of the OEM providers will use our technology as opposed to Microsoft s because of its ease-of-use for the individual consumers. We think those things position us well. Time will tell. I would rather compete with a real product than compete with a press machine. Tim Klasell - *Thomas Weisel Analyst* Maybe you can hit a little bit on the service providers, the ISPs of the world. Obviously McAfee has done a relationship with AOL. Is that a route to the consumer that you think is important? Or how do you think the ISPs may change the dynamics of the game? John Thompson - *Symantec CEO* We think it is an important route to market but we don t think you should view us as a philanthropy. We are a for-profit software company and therefore what I call Barney deals, where everybody feels good but nobody makes any money, is not the kind of market we participate in. So while AOL and McAfee may feel good, I am not sure they have delivered much to the bottom line in either particular case. Our relationship with companies like Tiscoli, like P-Online (ph), like EarthLink, like Yahoo!DD (ph), all been about (technical difficulty) both make money helping consumers secure their online experience. You should expect to see us continue to play in deals where there is a mutual win-win opportunity for us and the service providers. We don t think that changes the tenor of how consumers will get their security technology. Consumers acquire technologies, particularly software technologies, first through what is preloaded on the device by the OEM manufacturer. Hence that is why our strategy of focusing on the OEMs is so important, not just in terms of what happens with Microsoft, but also what might happen with other channels as they try to disintermediate us to a particular buyer. We will continue to focus on strategies where selling to service providers and having them in turn sell to end-users, will deliver win-wins, revenue and profit opportunities and it is unlikely anytime soon that you re going to see us do Barney deals just to have press releases and feel good stuff show up in the press. I just don t believe in that. Tim Klasell - *Thomas Weisel Analyst* Very good. We sort of go down that path, the consumer, the home gateway, there is a new opportunity, probably perhaps of a little bit of a risk to you. How do you plan on addressing that as we are seeing 60 percent of broadband homes now have a home gateway? streetevents@thomson.com 617.603.7900 www.streetevents.com 7

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

John Thompson - *Symantec CEO* It depends a what you define as a home gateway. If you define a home gateway as nothing more than a firewall that protects the access point into the home, then clearly we will participate in that market. The question becomes however, what is the route to market because in many instances it is low end VARS (ph), it s people like the folks who have done the engineering in my home who come in and preinstall a set of products just for the purpose of providing gateway access and protection at the same time. It is our believe that there is an opportunity here that is more appliance based and so the question becomes what are the economics associated with the model? They clearly aren t the same attractive economics as the software business and so we continue to look at it and look for ways to get our software into those products as opposed to being the hardware provider itself. Tim Klasell - *Thomas Weisel Analyst* Very good. Less than 5 minutes, so if anybody in the audience has a question I highly recommend . All right, the appliance model. You have been doing very well with the 5400 and some of your you have introduced your 8000 series. How much of a security and (indiscernible) backup world do you think will go to the appliance model? How much do you think will be an addressable market that you laid up there, 56 billion, do you think will end up being a software market? John Thompson - *Symantec CEO* It is our belief that the gateway tier will overtime be dominated by the appliance platform because it is an easier way to install and manage, if you will, the various types of sensors that need to be deployed at the gateway. What is called UTM, our unified threat management category, is the fastest-growing category of security technology sold today. You re going to see many, many companies continue to want to enter that market because they see it as a high-growth opportunity. We believe that in the mail environment you can in fact build, purpose-built boxes, that will focus on not just content filtering but spam filtering, and shaping the traffic flows into and out of an organization. The 8100 and 8200 products are designed with that in mind. That is provide content filtering for worms and viruses as well as spam and also shape traffic. So if you see a flood of email coming from a certain part of the Internet, constrict the flow of traffic such that a network does not get overloaded, if you will, by that traffic. Those of the kind of opportunities that we think lend themselves very, very well for appliances but we re not from the school of thought that says everything goes appliances or everything stays software. I think customers want the flexibility to be able to choose which implementation model they want and so you will see us deliver both software as well as appliance form factors depending upon the nature of the opportunity. Tim Klasell - *Thomas Weisel Analyst* Very good. So the next question. The latest hot topic out there in security is obviously spyware, and obviously Microsoft has released some product. You re going to be introducing some product fairly soon. The dynamics here are if Microsoft has introduced a product and they are not charging for it right now, even though you introduce a new product do you think you would be able to charge for it? (multiple speakers) the dynamics would be in that market? John Thompson - *Symantec CEO* In the spyware market, the most pervasive technologies deployed today are free products yet there are companies that sell spyware offerings in the marketplace. So the fact that Microsoft is in the market is interesting, but it does not destroy the market in terms of it having a real price to value relationship. So the question becomes, to what extent can we deliver something that is better than what Microsoft does to the point where it is better integrated with other functionalities we have and consumers or businesses are willing to pay for that. We think there is a temporal nature associated with this market which is there is a moment in time, a period of time, in which you will be able to charge the consumer or the business user for spyware, but a specific spyware solution. But there will come a point in time when they will want all of the malware detected by one engine and one capability. So it s take advantage of it now while the market is there, recognizing that over time it might in fact go away. streetevents@thomson.com 617.603.7900 www.streetevents.com 8

FINAL TRANSCRIPT SYMC Symantec Keynote at Thomas Weisel Partners Tech 2005 Conference

Tim Klasell - *Thomas Weisel Analyst* When you introduce your spyware product, can you give us an idea of where those price points might be? Will it be in line ? John Thompson - *Symantec CEO* Nope. We don t preannounce prices before we deliver them to our channel partners. So you should expect to see us deliver a product this quarter for the consumer market and this quarter for the enterprise markets. And when we announce those products that is when we will announce the price. Tim Klasell - *Thomas Weisel Analyst* Okay. John Thompson - *Symantec CEO* Good try though. Tim Klasell - *Thomas Weisel Analyst* I had to ask. Maybe I can narrow you down a little bit on the (indiscernible) for this quarter. We ve got 6 weeks left. John Thompson - *Symantec CEO* One of our OEM manufacturers, our partners, should be getting a drop here very shortly. So the way this is going to rollout is it will first show up in one of the OEM partners and then another OEM partner gets another drop because they each have unique configurations of what they do. Then you ll see a packaged product. And so the visibility base will be a function of when the OEM starts to ship that image, but one of them already has a couple versions of the product going. Tim Klasell - *Thomas Weisel Analyst* Very good. Thank you very much, John. John Thompson - *Symantec CEO* My pleasure. Thank you. DISCLAIMER Thomson Financial reserves the right to make changes to documents, content, or other information on this web site without obligation to notify any person of such changes. In the conference calls upon which Event Transcripts are based, companies may make projections or other forward-looking statements regarding a variety of items. Such forward-looking statements are based upon current expectations and involve risks and uncertainties. Actual results may differ materially from those stated in any forward-looking statement based on a number of important factors and risks, which are more specifically identified in the companies most recent SEC filings. Although the companies may indicate and believe that the assumptions underlying the forward-looking statements are reasonable, any of the assumptions could prove inaccurate or incorrect and, therefore, there can be no assurance that the results contemplated in the forward-looking statements will be realized. THE INFORMATION CONTAINED IN EVENT TRANSCRIPTS IS A TEXTUAL REPRESENTATION OF THE APPLICABLE COMPANY S CONFERENCE CALL AND WHILE EFFORTS ARE MADE TO PROVIDE AN ACCURATE TRANSCRIPTION, THERE MAY BE MATERIAL ERRORS, OMISSIONS, OR INACCURACIES IN THE REPORTING OF THE SUBSTANCE OF THE CONFERENCE CALLS. IN NO WAY DOES THOMSON FINANCIAL OR THE APPLICABLE COMPANY ASSUME ANY RESPONSIBILITY FOR ANY INVESTMENT OR OTHER DECISIONS MADE BASED UPON THE INFORMATION PROVIDED ON THIS WEB SITE OR IN ANY EVENT TRANSCRIPT. USERS ARE ADVISED TO REVIEW THE APPLICABLE COMPANY S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS. 1009194-2005-02-07T17:25:58.023 streetevents@thomson.com 617.603.7900 www.streetevents.com 9