

VERITAS SOFTWARE CORP /DE/

Form 425

March 09, 2005

Filing pursuant to Rule 425 under the Securities Act of 1933, as amended, and deemed filed pursuant to Rule 14a-12 under the Securities Exchange Act of 1934, as amended

Filer: VERITAS Software Corporation
Subject Company: VERITAS Software Corporation
Commission File No. of Subject Company: 000-26247

The following communication contains forward-looking statements, including statements regarding industry trends, such as supplier consolidation and growth in security attacks, benefits of the proposed merger involving Symantec Corporation and VERITAS Software Corporation, such as improved customer and platform coverage, improved product capabilities and lowered customer costs, post-closing integration of the businesses and product lines of Symantec and VERITAS, future stock prices, future product releases 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 the statements in this communication. Such risk factors include, among others, deviations in actual industry trends from current expectations, 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, difficulties encountered in integrating merged businesses and product lines, 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 communication. Additional information concerning these and other risk factors is contained in the sections of Symantec's and VERITAS' most recently filed Forms 10-K and 10-Q entitled "Business Risk Factors" or "Factors That May Affect Future Results." 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 article.

Additional Information and Where to Find It

Symantec Corporation has filed a registration statement on Form S-4 containing a preliminary joint proxy statement/prospectus in connection with the merger transaction involving Symantec and VERITAS with the SEC on February 11, 2005. Any offer of securities will only be made pursuant to a definitive joint proxy statement/prospectus. Investors and security holders are urged to read this filing (as well as the definitive joint proxy statement/prospectus when it becomes available) because it contains important information about the merger transaction. Investors and security holders may obtain free copies of these documents and other documents filed with the SEC at the SEC's web site at www.sec.gov. In addition, investors and security holders may obtain free copies of the documents filed with the SEC by Symantec by contacting Symantec Investor Relations at 408-517-8239. Investors and security holders may obtain free copies of the documents filed with the SEC by VERITAS by contacting VERITAS Investor Relations at 650-527-4523. Symantec, VERITAS and their respective directors and executive officers may be deemed to be participants in the solicitation of proxies from the stockholders of Symantec and VERITAS in connection with the merger transaction. Information regarding the special interests of these directors and executive officers in the merger transaction is included in the preliminary joint proxy statement/prospectus of Symantec and VERITAS described above. Additional information regarding the directors and executive officers of Symantec is also included in Symantec's proxy statement for its 2004 Annual Meeting of Stockholders, which was filed with the SEC on July 30, 2004. Additional information regarding the directors and executive officers of VERITAS is also included in VERITAS' proxy statement for its 2004 Annual Meeting of Stockholders, which was filed with the SEC on July 21, 2004. These documents are available free of charge at the SEC's web site at www.sec.gov and from Investor Relations at Symantec and VERITAS as described above.

The following is a transcript of the keynote speech given by John W. Thompson, Chairman and Chief Executive Officer of Symantec Corporation, at the Lehman Brothers Global Software, IT Services and Internet Conference on March 8, 2005:

* * *

Final Transcript

Conference Call Transcript

SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

Event Date/Time: Mar. 08. 2005 / 3:30PM ET

Event Duration: N/A

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

CORPORATE PARTICIPANTS

John W. Thompson

Symantec Corp. CEO

PRESENTATION

Israel Hernandez Lehman Bros.

(technical difficulty) (CALL IN PROGRESS) made a number of strategic acquisitions to enhance its ability to serve and rapidly change security and management (indiscernible) enterprises.

In September of 2002, President Bush appointed John to the National Infrastructure Advisory Committee to make recommendations regarding the security of the critical infrastructure for the United States. In addition, John has served as the Chairman of the Silicon Valley Blue Ribbon Task Force on aviation security and technology to identify and evaluate technology-driven solutions to further security and efficiency of national and local aviation. Prior to joining Symantec, John had a distinguished career at IBM where he held a number of senior executive positions in sales and marketing and software development. In his last assignment there, he was General Manager of IBM Americas and a member of the company's worldwide management council. John is a member of the Board of Directors of UPS, MySource and Seagate. He completed his undergraduate studies at Florida A&M University and holds a Masters degree in Management Sciences from MIT Sloan School of Management. Please welcome John W. Thompson, CEO of Symantec. (APPLAUSE).

John W. Thompson - Symantec Corp. CEO

Thank you very much. Thank you very much, Israel, and good afternoon, everyone.

I'm going to spend my time with you this afternoon talking about our view of where the industry is going and most importantly, Symantec's response to that set of trends and possibilities. Clearly, it's important that you understand why we are doing what we're doing. Once I'm finished with my planned remarks, you'll have an opportunity to perhaps ask questions, and I will give you the most crisp answers I possibly can.

However, before we go, let me remind you that some of the things I will say here are, in fact, forward-looking statements. Therefore, I would strongly recommend that you take a look at our published Qs and Ks for greater detail, and a way in which to bridge the gap between perhaps our GAAP results and the non-GAAP results that we often report.

Furthermore, we are involved in a transaction with VERITAS. That transaction we expect to close sometime during the second quarter of this calendar year. There are a series of filings that will occur as a part of that process, and we would also encourage you to review those filings so that you understand our view of the transaction and its relevant merits.

So, where is the industry going? We think there are 5 mega-trends that are in fact driving toward customers and therefore we as servers or participants of customers have to deal with, the first of which is customers' desire to deal with fewer vendors in the overall IT space. Clearly, the notion that I'd like to be able to get more of the technologies from a single supplier are real. In the security domain alone, there are hundreds and hundreds of companies that provide technologies yet, in many instances, customers find that they aren't as secure as they had hoped, once they had started down the path with 1 or 2 vendors. Therefore, consolidation is inevitable as customers think about better integration between product functions.

Second, clearly services are a significant driver to the exploitation of the software technologies that customers around the world will in fact avail themselves of. In the security domain in particular, because of the shortfall in skills, services are a very, very important complement to our software portfolio. So it is our belief that to be an effective solutions provider for infrastructure protection and availability technologies, we have to have a services complement to go along with our software business.

The third big trend is all around wireless. While clearly there will be a broader wireless infrastructure that will be delivered over time, the real issue is how will those wireless endpoints in particular be managed? They will introduce a new level of complexity to the customers' operating environment at a level of complexity that will not only have to be assured or secured but also better managed. It might mirror, quite frankly, many

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

of the early experiences that some of us will remember from the PC era, early days in the PC era, or were early days in the client/server era when

of the early experiences that some of us will remember from the PC era, early days in the PC era, or were early days in the client/server era when the investment in rapid application development made it possible for customers to do things that they hadn't been able to do before. The reality is the cost to manage all of those devices in many respects became more daunting than they had originally assumed.

The fourth area is one that is particularly relevant to the business that Symantec is in and the expansion plans that Symantec has, and that is all around Linux. Linux is an operating environment that has, in fact, garnered a fair amount of success for server-based applications in large enterprises. What Linux does for sure is ensure that the large enterprise environment will be more heterogeneous, not less. The fact that it will introduce yet one more choice of a platform certainly does offer the opportunity for Symantec (technical difficulty) as a pure play software company to deliver common tools across a broad range of environments. Furthermore, it's inevitable that there will be a competitive alternative to the Windows desktop environment driven by Linux. The question is not if; the question is when, because there are classes of applications that do lend themselves in the large enterprise environment to a Linux-based desktop. The question becomes, how do you in fact facilitate that migration for your operating environment and your company?

Finally, given the fact that scale is important to customers, hence trend number one, there will be more pressure for those of us in the industry to look for an opportunity to aggregate our capabilities, hence consolidation is inevitable. This is an industry where its growth rates are starting to mature or slow a bit, and hence aggregation and consolidation will lead to better customer options and alternatives and perhaps better alternatives for investors in their various companies as well.

These 5 big trends we believe have been a driving force in the industry for the last 24 months or more, and these 5 trends are in fact the things that we have been responding to as we think about our company and its strategy.

We started to articulate, in the early spring of I'm sorry, late fall of 2003, a view that says the marketplace will in fact converge, that there are domains of activity around the network, the storage and the systems environment where security is a part of all of them and we will have to deal with that obvious convergence. We recognize that, in our security business, intelligence about what's going on in the network world will in fact be an important determinant as to what operational actions customers will take to protect critical data. We also know that, to the extent that you can automatically push a software patch or reconfigure a server, you can in many instances make that environment less vulnerable or less susceptible to a particular attack. It's our belief that this phenomena will accelerate over the next few years and hence, how we position our company to take advantage of that phenomena is what we are all about today.

So, the key trends in this infrastructure arena are fivefold. First, there is no lessening of the number of digital assets that will be deployed by individuals and large enterprises. Today, many of us have, in digital form, not just our financial records but many of the things that are important to us about managing our day-to-day lives with our families, our MP3 players, our photo albums, all of which are now stored in digital format online. The fastest-growing segment, quite frankly, of the technology sphere these days is that of storage and storage management software for dealing with both personal and large enterprise assets that are growing exponentially.

Next, it is clear that what we're doing is becoming more complex. As customers put more systems in place, more applications, more users and more vulnerabilities are discovered every day, it's clear that this

heterogeneous environment that we have built will in fact have to be rationalized and made less costly to implement. The cost associated with becoming more compliant or remaining compliant with the evolving compliance standards, either be they horizontal standards like Sarbanes-Oxley or vertical requirements like Gramley Riley (ph), clearly will drive IT organizations to respond to the compliance initiatives that are becoming much, much more challenging today. We think that the issues around regulatory compliance will drive a reassessment of how the IT infrastructure is being built and managed and will force large enterprises in particular to think about how they operationalize many of the compliance initiatives, such that software is a part of the determination of whether or not you are or you aren't in compliance.

Finally, in our domain of security, it's clear that the frequency and complexity of the threats is not becoming less so. Today, a software vulnerability is exploited in about less than 6 days; it's actually 5.8 days from the discovery of a vulnerability to the time of exploit. While there have not been many of late very high-profile outbreaks, the number of Level 3 attacks continues to grow exponentially, hence the need for a more holistic approach to securing and managing the IT infrastructure.

Let me put in context one of the triggering events, at least for us, that forced us to think through our strategy and the implications of what technologies and services we should deliver in the marketplace. About 12 months ago, the average time between the discovery of a vulnerability and the release of an exploit was about 6 months. Well, in the case that is outlined here, this is the scenario for the Slammer attack. The Slammer attack occurred in January of 2003 when, in fact, a vulnerability had been discovered in the Windows operating environment in the July of 2002 time frame. At the moment in time that that vulnerability was discovered, literally people had 6 months between discovery and exploitation to do something about the operating environment that they had created. But to our dismay, customers chose to ignore that because the critical

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

vulnerability in the SQL server environment delivered by Microsoft caused many of them to find themselves incapacitated, if you will, at the moment of the attack.

When Slammer hit, literally every 8.5 seconds it doubled its infection rate. Literally within 10 minutes, more than 300,000 systems around the world had been ravaged by the attack. It was a server-based attack, not a desktop-oriented attack and therefore, as a result, air traffic control system didn't work; airplanes didn't get scheduled; ATM networks didn't work around the world. The resulting economic impact on the society in which we live was greater than \$1 billion. Yet, we had 6 months warning between the announcement of the vulnerability and the delivery, if you will, of exploit code to that vulnerability.

If customers had done simple things like push a software patch, they might have been able to mitigate much of the risk or damage associated with that attack. If they had done even more simple things like reconfigure a device on the network at the time that they saw the attack occur, they literally could have stopped this attack in its tracks before it doubled or accelerated its infection rate. So from this analysis of this attack, it became apparent to us that our strategy needed to evolve to be more holistic and it needed to include not just protection technologies but operational provisioning tools that would allow a customer to manage the infrastructure, both the applications and the devices that are on that environment, much, much more succinctly.

That is it is out of that understanding that VERITAS transaction was born. Now, interestingly enough, leading up to the transaction with VERITAS, we acquired PowerQuest, a small Windows-based server and backup systems company in November of 2003. In February of 2004, we acquired On Technologies (ph), a Windows-based server and desktop provisioning company that had recovery tools for configuring devices, for software distribution, for asset tracking, all of which led to a wonderful capability in the Windows environment but no single large enterprises Windows only. Hence what VERITAS adds to the Symantec product portfolio is richness in all of the variants of UNIX and all of the variants of the Linux operating environment, all of which over time will be prevalent in many large enterprises. So now we have the most complete software stack for security and availability in a multi-platform environment for large enterprises.

If you look at the capabilities that the combined company will bring to the market, there's very little overlap in the product portfolios, which we think makes this transaction's implementation a heck of a lot easier than one where there is enormous redundancy in products and therefore architects and engineers have to rationalize whose child or prodigy is better than the other. In this case, we have minor backup in the minor overlap in the backup space of the low end of the Windows marketplace. Clearly, VERITAS is the market leader in backup and recovery. We have some capabilities that came from our PowerQuest acquisition for what's called bare-metal restore, where you can not only backup the storage device but you can literally recover and restore the applications and the systems that are riding on the server itself. So very, very complementary capability. Today, we think the opportunity to leverage security and availability is what many of our customers are very, very interested in doing.

There are 3 areas of opportunity that we see right off the bat. One is around creating an environment where the infrastructure on which applications ride is more secure, more stable. That we refer to as the resilient infrastructure. Another is around the e-mail environment, where e-mail has become the mission-critical application for many large enterprises and in many sectors of the economy not just securing and keeping malicious content out of e-mail, but ensuring that you have archival and retrieval capability for that e-mail infrastructure are almost as important as the mail itself. Then finally around regulatory compliance, where with both the systems assets that have to be compliant as well as the

security exposures that have to be rendered explicit, we think there are great opportunities for the 2 companies combined.

So let me posture with you a few what-ifs. So imagine we see a new vulnerability on the horizon. With our BugTraQ infrastructure and the DeepSight alerting service that we offer to customers around the world, we literally see almost every vulnerability at the time the discovery, certainly at the time that it is posted in BugTraQ. We do an analysis of that vulnerability, and we can do 2 things 1, deliver a generic exploit-blocking capability so if it is ever exploited, the capability would prevent it from being devastating to customers. But 2 and perhaps most importantly is trigger a response to customers that alerts them to the vulnerability and give them ideas of triage strategies that they should implement to make sure that their systems are less vulnerable to the attack. Instantly with that alert, they could issue a backup message that says, issue more frequent backups of the data environment such that, if it does get attacked, the recovery time is much shorter. Because the real issue for most large enterprises is not if they are going to have a systems outage or an attack; it is when they do have one, how quickly can they restore to normal operations? We think this notion of tying alerting capabilities to operational provisioning tools for backup recovery, server configuration management will go a long way to helping applications be more available, which is what most large enterprises are most concerned about.

Another in the e-mail world clearly, with the acquisition of Brightmail and TurnTide, we have the best assets for managing the flow of mail into an enterprise, both eliminating malicious content from that flow of mail with our AntiVirus technologies, as well as dealing with the vexing problem of spam where, today, it represents something north 60 or 70 percent of the total mail traffic flowing through a network. So the idea is to

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

screen as much of the mail as possible on the front end, both for unwanted spam-like activity as well as for the normal malicious activity that would be associated with AntiVirus.

Now, with the combination of the 2 companies, we have the ability to further categorize what mail is coming into the environment and have intelligent archiving capability to store that mail based upon user type, domain or whatever the definitions might be for that particular enterprise, making it easier to retrieve those e-mail messages in compliance with whatever the regulatory standards or compliance standards might be for a given company. So, combining mail archiving and retrieval with front-end cleansing tools and security tools is a wonderful way to create a more complete mail security environment that is, in fact, more robust and more secure.

Then finally, with the never-ending unleashing of new regulatory standards, be they the horizontal ones like we deal with here in the U.S. or in Canada, or the vertical ones that are specific to a financial services or a healthcare, having tools that can substantiate those compliance requirements in software is a wonderful, wonderful way to facilitate automatic inspection and detection of compliance irregularities. Our market-leading solution called the Enterprise Security Manager clearly does position Symantec in a platform of strength for large enterprises, but now we can take that a step further and attach compliance for the operational side of a business, not just for user access or device access. We believe these things, when strung together, can in fact make next year's hopefully Sarbanes-Oxley compliance for some IT organizations a bit less onerous than it was perhaps in 2004. Rather than cloak ourselves in Sarbanes-Oxley, we'd rather cloak ourselves in the set of tools that surely will facilitate easier compliance admission by companies than what we've seen in the past.

We think the portfolio of the combined company, with market-leading technologies in 8 to 20 software categories, positions Symantec not only to lead where we are today but lead in areas where customers will in fact have more significant challenges in the future.

One of issues that I get asked quite often about how we will approach the integration is how will the sales integration model work? Today, each company has a set of tiered account structures and relationships, starting with, in the case of VERITAS, about 15 to 20 global accounts that are managed globally and Symantec with about 10 that are managed globally. We will, in fact, have a global accounts structure and national accounts or enterprise accounts that will be responsible for covering the large enterprise opportunity. We will be no less channel-friendly after this merger/integration than we were before. What that means is that Symantec will continue to use the channel as a very, very important fulfillment agent for whatever we do across the accounts structure. That is true for VERITAS more so in Europe and in APJ than it is in the U.S., and the fact that Tom Kendra will be the new sales leader for the combined company and Steve Messick will be the new leader in the U.S., Lindsey Armstrong will be the leader in Europe, and Steve Leonard will be the sales leader in APJ. We are in the midst of a rather significant rollout of all of the organizations for the new company. Most of what we call tier 1 and tier 2 have been named already, tier 1 being those reporting to me, tier 2 being those leaders reporting to those who report to me. We would expect to have much of the organizational activity completed by the end of the month of March. As a matter of fact, much of that through tier 3 will be done by next Wednesday, and we will have some of even tier 4, if you will, done beyond that.

So this is an important area for us with lots of focus. Our IMO or our Integration Management Office meeting of yesterday focused on the product portfolio and roadmap. The one that we will have on Saturday yes, Saturday will focus on the sales and go-to-market side for a full day.

We have had wonderful reaction from customers, partners and our employees. We've had a less-wonderful reaction from some of you. That being said, we are not deterred. We will continue to pursue this because we believe this is right for our customers and therefore right for our business.

Just recently at the RSA conference, I was joined by 4 very important customers who talked about their view of how security and available come together. Candidly, we were all encouraged by what they had to say.

So let me talk about the transaction and its timeline. It was announced for us on December 14. We announced it ourselves on December 16, at which point we said that we would expect to get the transaction done some time in the calendar second quarter of this year. We are still on track for that to occur. It is more likely May, mid to late May we think. We've cleared the regulatory footwear hurdle for Hart-Scott-Rodino in the U.S.; we are still in the process in Europe and we are awaiting comments from the SEC from our S-4 that was filed about 20 to 21 days or so ago, maybe a little bit less or more than that.

It's our expectation that, once we have comments back from the SEC, that we can in fact move quickly to release the proxy statement. We'd like to have that in the marketplace sometime in the late March/early May - late March/early April timeframe for a shareholder vote that will go on April and May. Assuming a close in the second quarter, we will be in full operations with a stub (ph) period, if you will, in that calendar second quarter that we will have to manage our way through.

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

The prior 12 months of activity for this company would look like a company that generated about \$4.5 billion in revenue. It had an operating margin, a gross margin that was approaching 85 percent. It had operating margins that were a little above 30 percent in aggregate and had an enormous, enormous generation of non-GAAP net income a very powerful software company with incredible cash-generating capabilities on its own right.

Our cash balance through the last 12 months was about \$5.5 billion. There's no reason to think that there wouldn't be some net add to that between now and the time that we close for sure with a very strong deferred revenue balance on Symantec's side, giving us very, very good visibility into a particular quarter. We cleared our convertible debt offering back in, I guess it was the September quarter, so Symantec carries no debt. Much of what's on the books for VERITAS is associated with leveraged leases and things like that on facilities that they have. The combined entity, by the time we open for business, will have somewhere between 13 and 14,000 people worldwide operating in about 41 countries with a phenomenal footprint of coverage, if you will, to the global market.

If you think about the aggregate business as it rolls up, since April of 1999, we have been focused at Symantec on having our revenue nearer the market. In other words, about two-thirds to three-quarters of all IT spending is done by corporate and government users. As we have thought about how we make Symantec relevant in the marketplace and less susceptible to vagaries in one buyer segment or another, having us nearer to market is important. Hence this new company will clearly mirror the market where about 25 percent of our revenues will come from the consumer business and about 75 percent of our revenues will come from the enterprise segment, if you will.

Furthermore, we will be a little less than I'd like to be in terms of U.S. or more than I'd like to be in terms of U.S. geographic revenue sourcing. Today, Symantec sits at about 48 percent from the U.S. market. We think, over time, the benchmark model is for the U.S. to represent about 45 percent of the total and therefore Europe and Asia representing the balance. We think Europe, as we open for business, is pretty close. Hence the growth opportunity for us is really in Asia as we get security and availability solutions better positioned in the Asian markets.

If you were to reflect on the guidance that we provided where we assumed an April close, there's no change to that guidance but let me restate here, which is, in the first 12 months of operations, we would expect a \$5 billion revenue stream; that's net of a deferred revenue loss of about \$300 million. We would expect operating expenses to run at about 55 percent of revenue. In our assumptions about earnings is an expectation of \$100 million in cost synergies to be derived, of which 13 million of that 100 will flow in the first quarter. The non-GAAP EPS outlook is 99 cents, and that is will be accretive; the transaction will be accretive in the first 12 months of operations, once we get this thing done.

We think we are bringing together we know we're bringing together the leader in security and the leader in availability solutions. We think what it does is address the issues of costs, complexity and compliance, which are clearly top-of-mind issues for our customers today. This clearly broadens the portfolio of both companies, giving us a heterogeneous software portfolio. It does not have a hardware agenda. Hence partners around the world and customers around the world are anxious to do business with the new Symantec.

This takes us from literally 6 years ago an addressable market of \$3 billion to, by the time we reach 2007, the addressable market opportunity for our new company will be \$56 billion. If we get our fair share of that, it certainly underpins the growth aspirations that we have for ourselves.

The sales model is we are I and Tom and Gary will spend a considerable amount of time on, between now and day one of operations, because we know that have to get that right in order to deliver the revenue. But when it's all said and done, when we deliver the revenue, we will have a company that can generate about \$2 billion in cash from operating activities and about \$2 billion in net income not a bad software company, I might add, one that if I were investing, I certainly would consider that.

So I will stop right there and see if I can't take your questions.

QUESTION AND ANSWER

Unidentified Audience Participant

(Inaudible question microphone inaccessible).

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

Final Transcript

Mar. 08. 2005 / 3:30PM, SYMC Symantec Keynote at Lehman Brothers Global Software, IT Services & Internet Conference

John W. Thompson - Symantec Corp. CEO

Well, software is a service that is really more about, in the main, the application that is being used by a consumer on the other end. So we could clearly perceive some of the security technologies that we offer to the consumer and small-business market being delivered as a service, as opposed to a software product in and of themselves.

That being said, we would also expect that our infrastructure technologies intrusion prevention, firewalling, policy compliance those things would be deployed by companies that offer that service to others, because they will need that to sustain the viability, if you will, of the infrastructure that they have had. So in consumer/small-business markets, you'll see us continue to deliver a service-oriented architecture over time but will be a license-based software company for infrastructure technologies either for customers or customers who want to deliver software as a service.

Unidentified Audience Participant

(Inaudible question microphone inaccessible).

John W. Thompson - Symantec Corp. CEO

I was either eminently clear or you are just tuckered out! Well, if there are no further questions, let me thank you for taking the time to hear our story and have a great conference! (APPLAUSE).

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 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. (C) 2005, Thomson StreetEvents All Rights Reserved.

Thomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com

(C) 2005 Thomson Financial. Republished with permission. No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Thomson Financial.

