VERITAS SOFTWARE CORP /DE/
Form 425
February 16, 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 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 these transcripts. 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 transcript. 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 these transcripts.

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 an address given by John Thompson, Chairman and Chief Executive Officer of Symantec Corporation, at the RSA 2005 Conference on February 15, 2005 and has been posted to a joint website hosted by Symantec and VERITAS Software Corporation as well as VERITAS internal website.

FINALTRANSCRIPTConference Call Transcript SYMC - Symantec at RSA 2005 Conference Event Date/Time: Feb. 15. 2005 / 10:35AM PT Event Duration: N/AThomson StreetEvents streetevents@thomson.com 617.603.7900 www.streetevents.com 1

FINALTRANSCRIPT SYMC Symantec at RSA 2005 Conference C O R P O R A T E P A R T I C I P A N T S P R E S E N T A T I O N John Thompson *Symantec Chairman and CEO* John Thompson - *Symantec Chairman and CEO* Good morning, everyone. And I truly want to thank Michael for such a gracious introduction. It s really quite an honor for me to be here to address the general assembly of the RSA Conference. While I was quite proud to represent Symantec a few years ago as we received an award for our innovation in the industry, this is the first time that I ve really had an opportunity to share with this audience our views of the industry and its overall direction. The truth is, in the early days of this conference, Symantec wouldn t have even been invited to participate. Viruses used to be rather a mundane thing, a problem that wasn t necessarily viewed as a security concern. And our company was clearly associated with consumer antivirus software, not the enterprise security challenge that many of you are facing today. So we ve certainly come a long, long way. Fourteen years ago the RSA Conference was little more than a convention of encryption enthusiasts. Now it s the most important conference in our industry, focused on the full gamut of security technologies. Just as one of you or none of us could have envisioned what would have happened to this conference a few years ago, nor could we have envisioned the tremendous growth that our industry would have seen and the development of this particular segment of the industry. In effect, this summit is a microcosm of that evolution. The agenda for this conference has transformed from cryptography to point product solutions to a full range of integrated security appliances and software. So I think that s an amazing transformation for a conference and a wonderful starting point for how I want to spend my time with you today.I could spend my time talking about Symantec or I could try to be like Bill and show you a demo or 2 of a product or show you our product roadmap. But I thought our time together would be better spent on a more strategic view of what we need to do as a group. I d like to take a giant step back from the here and now and pose a rather fundamental question to my security colleagues, a question like who are we? And what is the true value of what we do? So today I d like to explore the next steps that our industry must take as we redefine our value proposition to customers. I d like to push back on the paradigm that has defined how we as an industry serve our customers and reexamine what we do and how we get it done.First, who are we? Are we the chief security officer, the chief information security officer, the chief information officer or the chief risk officer? Whatever the label, security professionals today are front-and center of the IT organization and more attention and budget dollars are being dedicated to security and availability issues than ever before- Our role will change dramatically asstreetevents@thomson.com 617.603.7900 www.streetevents.com 2

FINALTRANSCRIPT SYMC Symantec at RSA 2005 Conference security concerns rise to the top of the IT agenda. It s already happening all around us. We will no longer just focus on protection Finally, compliance. That s the new elephant in the living room technologies, antivirus, intrusion detection or firewalls. today. I m sure all of you have or soon will be grappling with SOX 404 certification, not mention all the compliance requirements We will embrace offensive availability solutions as well as being thrust upon you by your specific industry regulations. It s configuration management, active in inventory tracking and becoming a regulatory alphabet soup; GLBA, HIPAA, to PIPEDA, recovery. And that s just the beginning. It s a brave new world and Basel 2, you name it. Needless to say, all of these bring their own our job is to pioneer how that world will evolve. It s not just about cost and complexity for you to deal with. technology anymore. It s about the information and the integrity that information has and its value to all of our users. It s about You can t avoid bumping against some new rule or regulation and ensuring a truly resilient infrastructure, one that can prevent an its information-based requirements, whether its records retention, attack or recover quickly in the event of an emergency or an discovery and retrieval, audible processes or security breach interruption. disclosure. Compliance has become a high priority item on the CIO agenda and it is wielding considerable influence on IT So I d like to talk about the challenges we face and investment decisions. It s no exaggeration to say that compliance how together as an industry we can successfully address them by has become one of the key challenges for the IT environment for delivering secure, available and integrated IT solutions. The the 21st century. challenges are all too familiar for those of you who ve been with me or as long as I have been in this industry. They are clearly the In this ever more complex, costly and regulated environment, it s 3 Cs, cost, complexity and compliance. Cost, of course, has always little wonder that you want to integrate the piece parts of your been the nemesis of every IT organization and while hardware infrastructure and you want to work with a strategic partner to do costs continue to come down dramatically, labor costs have been a just that. Now, I m not suggesting that you re going to do 1-stop real challenge for most organizations of late. With more systems shopping. None of us in the industry is that naïve to think that and applications being deployed, more security vulnerabilities you re going to buy everything from a single supplier. But your being discovered and more users to serve, the cost of delivering IT drive to address the basic challenges of cost, complexity and services is growing exponentially. compliance will be a significant factor in supplier consolidation in this industry over the next few years. I predict that in our The second challenge is complexity. Today you spend an marketplace we re going to see fewer vendors, better product inordinate amount of time managing the enormous complexity of integration, improved interoperability and fewer complicated your operating environment. Your world has become more license agreements to negotiate. In other words, fewer hoops and heterogeneous, not less. Not only do you manage traditional hurdles for you to clear. computing systems all over the worldwide network, but you re also seeing an influx of wireless applications and mobile devices. So let s spend some time on the solutions our industry must deliver You re managing the ongoing challenge of integrating architectures to make all of these challenges more palatable for you. Symantec and applications across a rather dynamic global network, while has been helping cu stomers for years solve security challenges, operating systems continue to multiply. from our simple beginnings in the largest segment of the industry, content security, to our introduction of the industry s first You re juggling Solaris, HP -UX, AIX, Palm OS, Symbian OS and integrated security appliance 3 years ago, right here at this very of course, Linux and a host of proprietary platforms from a broad conference. At the time, we inspired little more than widespread range of vendors. This heterogeneous environment ensures more naysaying. The industry pundits said, Customers just won t complexity, not less. Today the Windows environment is still the buy security solutions that way. most exploited and other platforms, including Linux, are now demonstrating similar weaknesses. And as these platforms And today, the trail we blazed is a well-trodden path as all of our continue to grow, you can be assured that attacks will follow. competitors have followed in our steps. There must be a dozen or so integrated gateway solutions on display here in the floor today. That s why we applaud Microsoft s security

initiatives. They are As a matter of fact, some well-known vendors are just now getting very necessary but, in my opinion, not sufficient for large around to introducing their own versions of what are now labeled enterprises. They don t offer a cross-platform heterogeneous unified threat management solutions . Notice how they dropped solution and genetically they may be incapable of doing so. That s the term integrated from their appliance description because they why Symantec and other purpose-built security companies don t really control all of the relevant technologies. I ll let you will judge for yourself whether unified provides the same level of always be a better alternative. We provide common tools across integration that we think you might need. the many disparate environments present in every large enterprise and we aren t distracted by computer games and a host of unrelated Just when competitors are catching up, the market s moving on; at security stuff going on. least that s how we at Symantec see the market. Our integrated

FINALTRANSCRIPT SYMC Symantec at RSA 2005 Conference security solutions have helped many of you take cost and Doctors rely on information to serve and diagnose patients. And complexity out of managing the security environment over the last utilities rely on information to supply energy. few years. Now we re looking to address cost, complexity and compliance across the entire network. Today we live in an information-based economy where data is not only an important currency, it increasingly is the product itself. Yet Today, we argue that it s more about integrated infrastructure information is under increasing attack and it s integrity is truly management, not just integrated security. It s about seamlessly being compromised. Not just from viruses and worms, but from a bridging the divide. Now, that s an important phrase, bridging the host of new cyber threats like spam and spyware, and phishing, as divide between security, device management, systems management well as the traditional array of natural or manmade disasters. and network management all across a heterogeneous environment because security, as traditionally defined, is no longer good We also know that the motive of the attackers is changing. From enough. We re in a different game now and with different rules and notoriety amongst a small group of friends to geopolitical power more stringent requirements. and fin ancial gain. Once the dust settled on Slammer, customers made it clear to us that we had to serve them differently. We had to The game changed with Slammer. It should have been a wakeup protect their information differently. It s not enough to make call for all of us to this new reality. It certainly was for us at information secure. We also need to make it always available. Symantec. Unleashed on January 25th, 2003, just a little over 2 Information that is secure but not available is useless. It s like years ago, the Slammer worm exploited a vulnerability in putting all your valuables in a safe and forgetting the combination. Windows-based systems that had been identified more than 6 months earlier. Slammer was aptly named; it slammed Windows Slammer shows us, or showed us that even when we as security systems, rendering them inoperable, doubling its rate of infection professionals got it right alerted companies to the impending every 8.5 seconds. attack, updated signatures and definitions, and recommended a response it just wasn t adequate. Traditional security wasn t It was the first of the so -called Warhol Worms, a reference to enough for Slammer. Even integrated security appliances weren t Andy Warhol s famous quip about 15 minutes of fame. Well, in enough. They couldn t ensure that your business would stay up and Slammer s case, it was just 10 minutes. It infected 90% of the running. unprotected systems or servers in just 10 minutes. Airline flights were cancelled, ATM networks stopped working, whole businesses Slammer delivered that loud message very clearly and gave us a shut down because of Slammer. And as soon as word got out that foreshadowing of what truly is to come. Today s threats move Slammer was in the wild, the mad dash began to quickly identify faster than ever before. It used to be that you had months to patch vulnerable IT assets, patch those systems and backup mission vulnerable systems. Today the average time for the exploitation of a new threat is less than 6 days. And that was 6 months that we saw in the case for Slammer. Once Slammer hit, companies struggled to bring their systems back online. In some cases, it actually took days to get that done. It Therefore new technologies, like the generic exploit blocking was clear that companies didn t know enough about their internal capability incorporated in our 7100 series of appliances, allow us environment to take t he immediate actions that they might have to deliver strong prevention capability ahead of the attacks. But our needed. They didn t have the necessary processes in place to researchers have been hard at work in an effort to stay ahead of the recover quickly. And in the end, the damage almost reached $1 attackers and making the process of managing security less costly billion worldwide, according to Computer Economics. That s the and less complex. We must shift our game to offense where we are cleanup cost alone. It doesn t even begin to account for the lost delivering an overall process for protecting critical information, productivity, lost revenue, lost trust or lost confidence of our not responding to threats or the most recent attack. customers. Slammer impacted the global economy in a way that we had never ever seen before and, in this case, there wasn t even a In other words, we must take an approach that is more proactive malicious payoff. and more holistic in protecting your information before it s compromised, stolen, infected, or misused. After Slammer, we So what s the most important lesson that

we learned from the realized that as we needed to be a strategic partner to our Slammer attack? Well, we learned that our industry view was customers and we must take a bold step. We had to connect much too narrow. We had too narrow a view of what our role as a external threat intelligence with internal knowledge about our provider should be and we learned we had to focus more on not customers infrastructure. just protecting the device or the network, but the actual information itself because information is the lifeblood of most An external early warning system provides valuable head starts organizations. Information is worth more that the piece parts, the when an attack is on the horizon. It s like seeing a big hurricane infrastructure, the databases, the applications, and the networks brewing on radar and knowing that it s going to hit in let s say 3 combined. Businesses rely on information to serve customers. hours. Good to know but short of scrambling to buy plywood and **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 4

FINAL TRANSCRIPT SYMC Symantec at RSA 2005 Conference duct tape, what can you reasonably be expected to do? Now The new Symantec, following the merger with VERITAS, will imagine if the radar tracking the hurricane s progress could talk to serve the full spectrum of customers from consumers to enterprise your home directly. And trigger the automatic activation of and governments of all sizes. We will operate at all tiers of the IT hurricane shutters or the basement sump pumps? infrastructure and on virtually every single platform. To truly protect your assets you have to be able to act on external One of the distinct benefits of this merger is our enterprise intelligence immediately, which means that your security system customers in fact will have a combined company that is a pure play needs to be able to talk to your internal asset management software company. So we have no hardware agenda. We can build capabilities, directly and on an ongoing basis. So imagine this anddeliver technology that will complement the existing scenario. What if an external threat alert could trigger an internal investments that you have in the hardware rather than force you to audit? You could instantly identify the systems that were replace them. vulnerable to attack. Take it a step further. What if the external alert could tell systems to access, assess patch levels on those In short, we can help our customers solve real business problems vulnerable systems and automatically update those that are with a focus on cost, complexity, and compliance. So let s take a unprotected? look at an area where we think there are wonderful synergies between security and availability, regulatory compliance. What if that external intelligence could prompt more frequent incremental backups in an end-to-end fashion from user systems Compliance is about understanding risks and developing strategies all the way up through the data centers? What if early warning to mitigate that risk. The compliance process requires protection could trigger an automatic sail over to a secure network andand remediation capabilities coupled with policy management prompt the restoration to a trusted clean safe when the threat solutions. Symantec already has tools and services that can help passes through the environment? information security professionals navigate the growing regulatory thicket and ensure compliance of their systems with today s And what if these actions could produce an audit trail to ensure security requirements. your policies and processes are in compliance? Now that I would assert, would be useful. Heck, it would be almost invaluable. So But an integrated solution also requires availability capabilities that the question for us at Symantec became how do we make this ensure that data is maintained from the end user level all the way happen? After Slammer, we realized we needed to strengthen our up through the data centers. It also requires cataloging and portfolio in the areas of access and storage management if we were indexing those capabilities for discovery and retrieval of to deliver this kind of integrated infrastructure solution. information. By combining our unparalleled security intelligence with device Sure you could cobble all these solutions together from various configuration capabilities we could help customers keep their vendors today, but getting this from one company focused on systems up and running no matter what. So we acquired integrating your infrastructure promises to improve security, PowerQuest and On Technology. These were not security enhance availability, and lower your overall costs. At the outset of companies. They specialized in backup and recovery and client and my remarks I talked about the transformation of the security server provisioning, asset inventory tracking, software distribution, industry. It s clear that we are no longer just security professionals. and patch management. Our goal today must be about mitigating risk. And the chief information security officer is typically the one tasked with that At this point, we could offer security and availability solutions to heady responsibility. our customers with one very important caveat. Our availability capabilities were predominantly in the Windows environment. And You re worried about the confidentiality, the integrity, and the as we all know, there is no large enterprise in the world that s availability of your information or data. You want to shield the Windows only, or few at least. To serve large enterprise customers, information you safeguard from threats. And yet you need to prove we needed a more comprehensive security and availability to regulators that you can produce accurate, auditable records upon portfolio. We needed to provide a truly integrated infrastructure demand. It s no longer a matter of technology. It s a matter of management

solution across all platforms. business process and in many instances business survival. It was out of this desire to fulfill customer needs that the merger In many companies this has clearly become a boardroom issue. with VERITAS was born, pure and simple. It marries the market The role of the CISO has clearly evolved to one with a broader leaders in both security and storage. Symantec already has the port folio and in much higher stature within the enterprise. Security broadest security portfolio or offerings in the market and the professionals have become strategic counselors to the business. merger with VERITAS will give us the breadth and depth to match on the availability side. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 5

FINAL TRANSCRIPT SYMC Symantec at RSA 2005 Conference At Symantec our CISO and his team don t administer security information technology and like the American frontier when the solutions. That s taken care of somewhere else in the IT country ran out of free land, when law and order had been organizat ion. established in the far reaches of the land and when the railroad shrank the country to a manageable size there is or was no turning Instead, they focus on strategy, defining standards, selecting back. The good old days are gone forever. So it is with our architectures, and establishing policies. They are responsible for industry. audit and compliance, making sure that our business units follow the processes they have defined. They focus on risk and its impact Our paradigm has shifted. Until today, we charted the frontier of on our business. the IT environment as security specialists. We patrolled the borders. We spotted the threats. We alerted those at risk. It s time to do As security professionals broaden their horizon and focus more on more. It s time to do more than raise red flags and block threats. risk, it s my strong belief that we ll see the CISO role evolve to Integrated infrastructure management means addressing all forms become the chief risk officer. Information risk is already taking of risk before they strike as well as after. It s about disaster center stage with the emergence of risk management groups to recovery. It s about systems availability. It s about proactive have over arching responsibility for information management protection of the entire infrastructure especially the information. across the enterprise. Our paradigm has shifted. In the old paradigm network We recently established our own internal global risk council, administrators could not see beyond their own parameters. They chaired by our CISO. This team includes people from across our couldn t sense an attack until it was upon them. In the new Company and they are responsible for assessing a broad range of paradigm they re armed with early warning intelligence that risks to our business and reporting the status of this work to the triggers security and availability countermeasures. In the old audit committee of our Board. paradigm network security was divorced from storage and systems management. Each had its own products. Its own people and even As a matter of fact, by 2007 Forester Research predicts that 75% of its own language. In the new paradigm the silos go away. More a large, critical infrastructure companies, those are healthcare and more we ll see integrated IT organizations with security institutions, transportation, telecommunications as an example. professionals playing an even more prominent role. They will all have established an enterprise level risk management office lead by a chief risk officer. Together we are redefining our In the old paradigm you were only as protected as you last update. industry. It s already underway. You and I can feel it. In the new paradigm sensors will prevent many of the attacks. And when they can t, alerts will trigger past distribution and Our role is truly evolving. No longer are we the custodians of provisioning and backups. So information stays secure and information security. We are the stewards of the integrated available and information technologists stay focused instead of infrastructure. Challenged with making it more secure and more fighting fires. available. The annals of commerce are filled with examples of companies that have transformed their model and in doing so In a world where our most valuable and vital assets information transformed their industry. Perhaps one that I know very well and roams the Internet where network walls no longer exit. Where the I m very familiar with is the example from the package deliver y threats to information are ramped and accelerating and regulatory business. demands for its security and privacy are incessant. We need to move beyond our security only focus and stake out our place in the In 1998 UPS embarked on a transformation that was as its CEO by information management category, but these are only the first steps described it s most radical in its 97 year history. They in a very, very long and ongoing journey. There s still more that we decided to redefine themselves and in doing so redefine their can do expanding our role to managing systems availability, industry. No longer was UPS in the business of small package network access and the performance of applications must be a part delivery or just small package delivery yet they concluded and of our mission. asserted they were in the global logistics and supply chain management business. Its new charter was to enable global In the end, helping our customers manage and protect the commerce, the flow of goods and information and funds on a global components that lie on top of all of that infrastructure. So leaders scale

internationally. Today UPS acts as the fulfillment center for don t follow and innovators often see ideas or opportunities where Nike.com. It s the repair center for Toshiba laptops. It even others can t. recycles many of your old computers and as the commercial says, there s an awful lot that brown can do for you. Fortune favors the bold. Those who take a proactive and comprehensive approach to ensuring the integrity of their I would contend that we re at a similar juncture in our industry s information and the resilience of its infrastructure. To get real lifestyle. A period where a redefinition of our roles is necessary. We value out of our information assets we must protect them. We must are at the cusp of an enormous opportunity on the frontier of **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 6

FINAL TRANSCRIPT SYMC Symantec at RSA 2005 Conference balance the need for availability with the imperative that we all have for security. Let s open our minds to the possibilities in our marketplace. Open our minds to the opportunities to grow as IT professionals, as companies and as an industry segment. At Symantec we intend to lead, to innovate and to be first movers in this wonderful industry of ours. I thank you for your support of our company and for the opportunity to share our view of where this industry s headed. Thank you very much. **D I S C L A I M E R** 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. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 7