VERITAS SOFTWARE CORP /DE/
Form 425
February 17, 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 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 this transcript. 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 this transcript.

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 a roundtable discussion in which John Thompson, Chairman and Chief Executive Officer of Symantec Corporation, participated at the RSA 2005 Conference on February 15, 2005 and which has been posted to a joint website hosted by Symantec and VERITAS as well as VERITAS internal website. Statements made by participants in the roundtable discussion who are not affiliated with Symantec or VERITAS should not be deemed to be attributed to or endorsed by either Symantec or VERITAS.

Final Transcript Conference Call Transcript SYMC Symantec at RSA 2005 Conference Event
Date/Time: Feb. 15. 2005 / 11:15AM PT Event Duration: N/A Thomson StreetEvents

Final Transcript SYMC Symantec at RSA 2005 Conference CORPORATE PARTICIPANTS **John Thompson** *Symantec Corporation Chairman and CEO* **Jon Oltsik** *Senior Analyst, Information Security, Enterprise Strategy Group* **Richard Jackson** *ChevronTexaco Chief Information Protection Officer* **Tom Jones** *State of California Department of Health and Human Services* **Rich Baich** *ChoicePoint Chief Information Security Officer* **Malcolm Kelly** *Reuters Global IT Security Director* **CONFERENCE CALL PARTICIPANTS David Bank** *Wall Street Journal* **Riva Richmond** *Dow Jones* **Jeff Englander** *Kaufman Brothers Analyst* **Carrie Kirby** *San Francisco Chronicle* **Curtis Schauger** *CIBC Analyst* **Tim Klasell** *Thomas Weisel Partners Analyst* **Garrett Bekker** *Tradition Asiel Securities Analyst* **Joe Menn** *LA Times* **PRESENTATION John Thompson -** ***Symantec Corporation Chairman and CEO*** Good morning or afternoon to everyone. I m John Thompson. I m the chairman and CEO of Symantec and I welcome all of you to this roundtable discussion. Ours is a wonderful forum for security specialists, both customers and solution providers to come together to talk about what s going on in our industry, how together we can do a better job of protecting the critical infrastructure that s been amassed around the world. And more importantly, where we think the industry s going. I have certainly have had my opportunity to share my views this morning and hopefully some of you had an opportunity to hear that. With me today are a number of experts let s call them that - from industry, both from the market analyst side as well as the user side, who will talk about this concept of security and availability. And while we at Symantec have been, for the last 18-24 months, suggesting to the market that there was a fundamental shift that had to go on, many of you have wanted your proof points of that, not just from Symantec s point of view, but from the point of view of users or people who truly are missioned with the responsibility for protecting critical assets that customers have deployed in their infrastructure. And so, what I d like to do is have these panelists give you a point of view and then open it up for questions after each of them has had an opportunity to speak. So, let me introduce each of the panelists to you and then we ll move on from there. First, from the Enterprise Strategy Group, is Jon Oltsik, to my immediate left. Next, the Chief Information Security Officer and a true security professional from ChoicePoint, Rich Baich. From the State of California, which is one of the largest state government users of information technology, from the Department of Health and Human Services, Tom Jones, and Malcolm Kelly, who is from Reuters, one of Symantec s very important customers and a very avid user of information security technologies. We certainly believe that these individuals are representative of how technology is being deployed today and, more importantly, are forward-thinking in their view of how technology will be deployed tomorrow. So, let me have Jon Oltsik set the context for this discussion this morning. Jon? **Jon Oltsik -** ***Senior Analyst, Information Security, Enterprise Strategy Group*** Thank you, John. Can you hear me? Is my mic on? Okay. So, I should start by saying this is just another day at the office for me because my days are usually spent talking to technology vendors and users and institutional investors. That includes calls here and there from the press, so, just another day. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 2

Final Transcript SYMC Symantec at RSA 2005 Conference But the subject matter is where is security going? How is the security industry changing. And I m a relative newcomer to the security industry. I ve been covering security for about 2 years now full-time. But in terms of where security is going, I have to say we ve seen this movie before. And those of who fit in the information technology industry for a long time will all say that. So, for instance, I started my career in 1987 at EMC Corporation. And back then, when we sold disk subsystems, what we sold was head disk assembly RPMs and we sold IO and we sold controller intelligence. And now, what the storage industry sells is information lifecycle management, so it s the management of data for business context. Is this data important? Where does it have to go? Does it need to be archived? Does it need to adhere to regulatory compliances? So, things like that. Later on in my career, I was very involved in system and network management. And at the time, what we d do is we d look at router portability and SNMP mid. And we d look at usage statistics. Well, now if you look at what s happening in network management and systems management, it s all about business process management. So, what I want is a tool that will give me a view of all of the systems, all of the networks that comprise some business process or critical application, and I want to use those metrics to help me make business decisions on SLAs, on performance, on capacity planning, things like that. So, when I got into security, I saw a number of point tools, I saw a number of disparate solutions, I heard a lot of talk about technologies and it just occurred to me, this has to change, this has to migrate to a much more business-centric industry. And what John said downstairs and what you ll hear throughout the day and on the show floor is we re in the process of doing that. That we really are changing information security to address business risk, not technology widgets. Are we there yet? Absolutely not. Absolutely not. Anyone who does what I do or what these guys do will tell you that just from our data, 66% of companies in a recent survey told us they were impacted by a worm in the last 12 months, in spite of the fact that there are technologies to help there. 14% of those said that the impact was severe. We re still getting troubled by this. Now, on the other side, on the Veritas side of the business, we know from our heritage which was in storage at ESG, 30-40% of backups fail. And it s for a number of reasons. This isn t a Veritas reflection. It s because of media problems, hardware problems, human error, configuration problems. But when backups fail, that means data is not protected. That means I lose critical data. That means that there are things that I can t do productivity-wise because the data is gone. So, when I m asked where is the security where is security technology going, I wrote a column in C-NET at the beginning of this year and I said this is the year of the BUT. And I don t mean that in an anatomical way. This is a 3-letter acronym. And so, B-U-T. The B stands for back. So, we know that 64% of companies still say that they have a high investment in perimeter security. The numbers drop down precipitously when you look at other areas. So, we have to get back from the perimeter. We have to protect critical assets wherever they live. And we have to protect critical data. And I can tell you that storage infrastructure is extremely insecure. So, the U in BUT stands for up. And what I mean there is up the technology stack. So, Port 80 is wide open, Port 25 is wide open. We know that those are attack vectors. We need to do a better job of protecting critical applications. And we re seeing some of those solutions come into play. But most companies or many c ompanies still haven t figured that out. We also need to write more secure codes, which is something that s a work in progress. And so, finally, the T in BUT stands for together. And this has a couple of meanings. One is we ve got to sell security solutions. No one can manage disparate (indiscernible). No one can manage disparatelog files. It s not giving us an enterprise picture. So, we need to address that very quickly. And the other thing is we need to integrate all these solutions and integrate them across so that, again, like the system network management guys, we get a business view of security for critical infrastructure and critical applications. So, let me just conclude by saying that in our research, we asked people to identify the type of traffic that was most vulnerable to attack. And unquestionably, people said e-mail. 46% of people said e-mail versus 22% for Web traffic. And so, clearly a problem. That John s company they have purchased BrightMail. (ph). They just put out a new appliance called the 8100, very deep inspection for spam and for antivirus. And Microsoft just

bought Sybari the other day. They realize this is a problem. But we know from what we do that it s impossible to manage user accounts in e-mail. It creates a massive storage problem. People don t back up Exchange like they back up their Oracle databases, so there s a lot of data that s unprotected. And a lot of the compliance issues require that data be archived. So, today on The Wall Street Journal, I saw that someone I think it was JPMorgan Chase, but I hope I m not wrong because I m saying this. But they were just fined $3.1 million because they didn t provide the e-mail evidence in a court case so they were liable. And they had to pay a $3.1 million fine. So, e-mail archiving is important, too. So, just to summarize, when you look at the e-mail environment, it s not about spam and antivirus. That s a piece of it. It has to be a comprehensive risk management solution for a critical application and that s where I see security going. It has to broaden. It has to get on the point tools realm and it has to be integrated for a business solution.

Final Transcript SYMC Symantec at RSA 2005 Conference John Thompson - ***Symantec Corporation Chairman and CEO*** Thank you, Jon. Let me introduce our next speaker, who I failed to introduce as I was going down the line. I apologize. He s Richard Jackson, the chief information protection officer for ChevronTexaco. Richard, welcome. **Richard Jackson -** ***ChevronTexaco Chief Information Protection Officer*** Good morning or good afternoon, whichever time zone you happen to be in. Let me give you a little bit of information about the scope of ChevronTexaco first, and then I d like to talk about something we call digital intensity. We ve got 52,000 employees who are out there in over 175 countries. We sight over 10 million credit card customers throughout the world. From an IT perspective, we have over 40,000 desktops in use. We have over 8,000 laptops, over 750 LINUX and UNIX servers. And we support about 1,800 locations, including 1 or 2 sales reps running around parts of Asia and Africa with a laptop and an Internet link back to the network. That s complexity. And that s also indicative of a lot of data that we collect and store and manage. ChevronTexaco operates throughout the value chain of the oil and gas industry. We explore, produce, ship, refine, market products on a daily basis. Let me give you some indication of what the role of the storage and information is in this value chain. At any given time, we ve got about 50, 3-dimensional (indiscernible) in place, generating over 350 terabytes of data that gets stored. We have 100 simulation models in effect, generating over 10 terabytes of information. A large oil field will have over 1,000 input-output measurement points. Our data strength can be 10 gigabytes per day per offshore field fields. Our large refinery has over 30,000 instrumentation input and output points and you know it s over a terabyte a year of process data. I m going to look at the value share a little bit more here. Our enterprise systems we have over 4 million commercial transactions per day handled by our ERP systems all of generates data that s stored and managed. Over 1 million e-mail transactions per day, excluding a lot of the spam that we filter out. Our internal network traffic is now at a terabyte a day. Relatively speaking, we saw about 500 terabytes of data stored currently throughout the world. Managing that data, securing that data, accessing that data is critical to our operation and our livelihood. So, the challenge that we see ahead of us is that, with this kind of storage, you have to be able to find what you need when you need it, which is availability. You have to be able to trust what you find and when you use it, which is integrity. And you have to manage control of who has access to it once you collect it and store it. And you also have to keep what you need so that you have it when you need it, which is a compliance issue. And you have to do all of this at an affordable cost. So, what s really important, from my perspective, safe reliable operations, we have to operating safely, not only from a security standpoint, but from a personnel and environment perspective. We have to maintain the integrity of the data. It has to be protected from unauthorized access, confidentiality has to be maintained and it cannot be altered. Decision quality is critical in our industry. When we make a decision, we make an investment, we live with it for 30 years. We cannot rip out an oil field or an oil platform. We have to live with it. The decision quality is critical, so the integrity of the data is paramount for us. Managing the lifecycle of information. We have to make good decisions on what data to collect, but once we ve done that, we have to store and retain it. And we have to be able to find it. I spend a lot of time looki ng for files on my hard drive. Maybe I m unique in that capacity, but I suppose that some of you have the same problem that I have, which is finding what I need when I need it and finding the right version of what I have. Cost control critical for us. We have to maintain tigher control on costs. So, let me leave you with a couple of parting thoughts. Our focus on cost control and optimizing the value chain drives our decisions on our business partners in many ways. Included are companies offering integrated solutions with a global support capabilities that align with and improve our business processes are what I look for. This is important to controlling costs because point solutions can be very costly. I personally look for companies with a great management team, a good track record and strong financials that transforms itself periodically, the lawyers remain relevant to the marketplace and a better sort of customers as well as its investors. Symantec certainly fit that description, so I m very much looking forward to seeing their strategies around the Veritas acquisition and what they bring to the table for the marketplace. Thank you. **John Thompson**

- Symantec Corporation Chairman and CEO Thank you very much, Richard. Now, let s move onto Tom Tom Jones. **Tom Jones -** ***State of California Department of Health and Human Services*** Hi. I represent the public sector version of this panel and we are not immune, believe me, even back in the days when all we had was a mainframe to rack up, we were still a little bit vulnerable. But one of the things I want to position you with is the size of the data center that we have at Health and Human Services. It s got about 150,000 customers. It has 2,500 routers. It has it represents 70 major departments that fall primarily, obviously, within the **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 4

Final Transcript SYMC Symantec at RSA 2005 Conference Health and Human Services. So, our protection requirements are focused, as you might imagine, towards the HIPAA regulations because we deal with a lot of electronic personal health information. And protecting that it s about 300 terabytes worth of data that we have. And it s very, very difficult. It s very we ve tried many, many different kind of tacks on how we were going to protect the data. We felt that it was important for us to deal from the perimeter and work our way in and I think that that s the wrong strategy. I think that we revisited now that the members of our, basically, security advisory counsel have said that it s probably more appropriate that we take a different view. Of course, if you listen to Bill, all we have to do is wait a couple more months and it sounds like all our problems are going to be solved anyway. But I think we probably are not going to look to the culprit for the solution, as least for awhile. Okay? So, that doesn t necessarily mean that I m anti-Microsoft product. Don t get me wrong. But I know that most of our problems seem to come from Microsoft attack exploits. One of the things that I think we ve done is that we ve moved away from scan and permit technology, especially in the area of IDSs to more proactive scan and lock. It s been around in AV forever. It s been around in firewalls forever. And what we ve decided to do is, at least at the perimeter and at various touch points within our network again, a very, very robust network it s 2,500 sites. All Cisco-powered, by the way. Is to actually place IPSs in line where we can actually do the best for our customers. We re working our way back from mission-critical servers all the way back to the perimeter and putting in that defensive depth strategy. One of the things that is particularly problematic for us, obviously, is because of HIPAA compliance issues is how you deal with secure transport. Obviously, in your Web applications, you have SSL opportunities, legacy applications that are using Passport and tools like that and have plug-ins that will actually give you either IPSec or SSL or AES type encryption, but also when you re dealing with the applications themselves, we re finding that most of the developers who are contractors, who may not even be around anymore, probably did not such a good job. We re using tools now to be able to scan those applications, determine if they re vulnerable for buffer overflows or crossite (ph) scripting or Tipo (ph) injections or broken wings and things like that and we re finding, to our actually that it s not as good as we had hoped. And so that means that there s a lot of reengineering on some of the applications that have actually been out there and could have been exploited over time. We re finding also that we need to have some kind of secure email. Mission critical services include email now. And so we ve got to look for someone who s going to be able to provide some way of being able to protect electronic protected health information as it s processed through email. We re looking at various point solutions. We think that Symantec actually has got a really killer solution when you match that Brightmail product that Richard just talked about or John just talked about with Voltage. We re really excited about that relationship and see if we can t actually provide it as a service offering to our customers. The data center itself gets hit with about 2.2 million attack signatures a month. And that seems like and we re pretty successful at blocking them. We ve got a very, very committed security advisory council, we ve got a very, very committed security operations group and so we re v ery passionate about this stuff. And one of the things that I d hope that in fact I could take exception with John on is the fact that maybe there is a silver bullet out there; maybe there is a single vendor solution. We had it when we deployed point solutions. We ended up with they re not integrated to the degree that we need, they re not scalable to the degree that we need, they more interface than integrate, user interface, system administration, a lot of these things become issues for us. We re hoping that in fact someone does emerge as the winner and we re very hopeful in that area. But one of the things I think is extremely important is that a couple of years ago I started coming to these shows and I used to ask the vendors, Listen, I got a problem because I provide extreme amount of VPN and ROV access. How can I block an infected asset from getting into my network and, at my direction, either let him in or not. And most of the vendors were saying, Oh, we can do that or We should be able to do that or No one s ever asked that. And so the key issue was for me not Slammer, it was Blaster because if you remember when Blaster came out now, you actually could have all the patches in place and still have an infected device. And so what I was trying to

say is since we have a lot of ROC and laptop users that are hitting our networks, how do I keep this guy out? Now we have solutions where before all we were getting was vendor lip service. And I think that s good, that s a trend. We see that. But I can tell you right now, also my personal experience, spyware is right now it s on the hype cycle, it is still hot. I took a completely naked machine yesterday, this is absolutely not the machine had never been on the Internet at all, it had been patched, it was current, we had 3 versions of spyware on there; 2 were real-time, 1 was the beta version of Mr. Gates product. And I got on there, went to 5 Websites, simply did copies of some JPEGs for a valentine that I was building, just little kitty cats, and when I got done I had 179 critical objects on the machine and 2 viruses and 1 Trojan. Now you figure that out. We re still not there yet. Anyway, that s where I think we need to throw our energy because that s the thing that s killing us. Not only is it going to kill everybody in this room, it s going to kill everybody out there, too. Anyway, thank you very much for your time. **John Thompson -** ***Symantec Corporation Chairman and CEO*** **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 5

Final Transcript SYMC Symantec at RSA 2005 Conference Well, few businesses are more information intensive than ChoicePoint and here from ChoicePoint is an old friend, Rich Baich. You re up. **Rich Baich -** ***ChoicePoint Chief Information Security Officer*** Thanks, John. I m going to take a little different approach. Let me take you back. If you go back to the 90s and you think about kind of the whole evolution of how the Internet and businesses have taken off, you ll quickly remember it was routers and switches and it moved to a network management system. And I think security is in the same transformational mode that network management was in the 90s. Now that we re here in the 2000s, you go back, in 98, 99, security began to hit the headlines, firewalls, couple of years later, IDS, antivirus was thrown in there, the marketplace continues to emerge, you ve got intrusion prevention, anomaly detection, security event management, all these different point solutions. And when you look at the life cycle of security, eventually it all has to come down to some type of managed system. And the management of that system is geared towards business operations. And the key point that I want to make today is it is not security, it s a business enablement. During the keynote, several people talked about many phrases, business survivability, technology adversity business, it s a very true battle. Out there among the executive ranks right now, one of the most difficult things is to be a leader, to be a change agent, to be a pioneer because we re working off a system that was established off of a CIO who came to light in the early 90s, then a CTO and now you have a CISO. Is CISO the right title? I think John did a great job of comparing the different names that are out there from security officer to risk management officer. Heck, it could be a compliancy officer as far as it goes. But the critical point is leadership. In the organization, positioning the security as a service enabler, as a business enabler is key. There s still a little bit of confusion when I actually talk about it being an infrastructure ploy. Whether it s infrastructure or not, it doesn t really matter. The key point is that an individual that has that responsibility, they have to stay focused on what s the value they bring to the organization. And that value is business enablement, enablement being defined as availability, enablement being defined as integrity of data or confidentiality. Regardless of the industry, there s a dependence on the Internet and that Internet somehow, some way, is taking information from each and every organization, whether it s email or whether it s database pulls, whether it s applications that perform analytics, but the key thing is that as leaders, we have to focus on making sure that availability is there. We have to change the way we talk. So many times you hear people talk about we re going to do a project. It s not a project; it s a business process. In general, I talk about security as 60% is process, 30% is people and only 10% is technology. The technology needs to come after the process has been defined and the people have been identified to ensure the survivability of it. So if you look at the way the marketplace is maturing, and I have to give Symantec kudos, availability is an important facet. If you look at the holistic approach to security, you have an asset. You have to know what it is. Once you understand that asset, you have to label it. And there s lots of different ways you can label it and we ll just make it simple and we ll say critical versus non-critical. From there you can then correlate a risk, what security posture do I need, what availability posture do I need, how important is the confidentiality and integrity of that inf ormation. And then from there you define a process and you choose a technology to mitigate the risks. But if you don t know the if you don t know what the asset is and you haven t taken the time to label it through a data classification program, classification program, then you re just spending money without thinking through the issue. And how do you come to that conclusion? It has to be a business decision. As a chief information security officer, I cannot stay in my office and make decisions; I have to go out to the business leaders to make sure I understand their business and let them understand the compliancy issues to the business that might relate back to the different regulations that are out there. Immediate response would be we re not regulated. Well, we re not regulated potentially, but our partners are regulated. So those regulations will filter down to us. Just because you re not a financial institution, if you do business with a financial institution, you basically fall on the GLBA because that s going to be a requirement to do business with them. So I think we have to look at how we re describing what we re doing. And in general, this is all movement towards a risk model. Whether you want to call it operational risk, compliancy or

just risk in general, the reality of it is risk is a business decision. Most organizations, if you mention who s the chief risk officer, who does risk management, you end up finding out it has to do with insurance or financial derivatives. So we have a language that we have to change. But the reality of it is what value that we bring as security executives to an organization deals with mitigating risks and ensuring that the risks meet customer demand. And those customer demands have a security profile, an availability profile and a requirement when it comes to confidentiality and integrity. So the intertwining of privacy, availability and security is really the same language, just different terms. And it s going to take ambitious change agent leaders to try to get that across. And one of our biggest problems is that corporate infrastructure and how do we translate that. So John, I want to say thanks and hopefully you ll carry that thought forward and help us get the respect, the empowerment that we need to transform security from a technology integration solution to a business enabler through risk mitigation. **John Thompson -** ***Symantec Corporation*** ***Chairman and CEO*** **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 6

Final Transcript SYMC Symantec at RSA 2005 Conference Thanks very much, Rich. Our last speaker certainly does represent an information intensive business. It s Reuters. And so Malcolm Kelly, welcome. **Malcolm Kelly -** ***Reuters Global IT Security Director*** Thanks, John. You have heard that information really is the lifeblood of most organizations but none more so than Reuters. We are an information company and we recognize the importance we play in providing accurate and timely news to the world. We always have journalists and photographers all over the world, major world events, major news events. And I haven t bumped into any yet, but I wouldn t be surprised if there were a couple hanging around RSA 2005. We re well known as a media news organization. Most of our revenue actually comes from financial services organizations. Again, we provide all sorts of systems and data to investment banks, insurance companies, and that data, too, has to be accurate and it has to be available when they need to use it. It has to be available. Indeed, many of the world s leading financial services organizations have built their own systems which rely on market data feeds from Reuters and other market data providers as well. And so those systems really at the heart of their business have to be available. You ve also already heard today about some of the regulatory requirements organizations face. Indeed, financial services organizations in particular also have to (inaudible) their supplies. Richard just mentioned it. But as an integral part of some of their systems then, that regulation compliance feeds down into the systems and the market data feeds that we provide these clients. So we ve an important role in playing in their organizations and demonstrating the compliance of their systems. Now information security professionals always worried about the confidentiality, integrity and availability of information as the famous CIA acronym. However, these disciplines have usually resided in different parts of an organization using different processes, different products, different source set. And the focus today within Reuters is on service. Service is our number 1 priority. But we also recognize that we need to have secure information feeds (ph), maintaining the right level of security. Too much security is just as bad as too little. So it is trying to achieve that balance between availability and between integrity. I strongly believe there is a place for suppliers (ph) to the information security industry to bring these aspects together, certainly the strategy Symantec progressing now is moving down that path and really interested in that. It s key for us at the moment in Reuters about service, about availability, but in also ensuring integrity. And in certain cases the confidentiality aspects around privacy, et cetera. Being able to deal with any of the threats to information that may materialize and it s not necessarily viruses and worms, it s also hardware failure, it s also acts of God . Being able to deal with invasion of privacy in a manner that maintains a resilient service is key to the best in the future for all of us. I know our clients expect that of us, so we in turn expect that of our suppliers. Thank you. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 7

Final Transcript SYMC Symantec at RSA 2005 Conference QUESTION AND ANSWER John Thompson - ***Symantec Corporation Chairman and CEO*** Thank you very much to all of the panelists. This is now your opportunity to ask questions of all of us here on the panel. And there are microphones that are around the room, so if you raise your hand someone will here s one. **Carrie Kirby** ***San Francisco Chronicle*** I apologize if you went over this before I entered the room, but was wondering what your reaction was to Microsoft s announcement this morning that their antivirus product will be coming out this year and that they re going to be giving away spyware for free. And also I was wondering... **John Thompson -** ***Symantec Corporation Chairman and CEO*** There s no new news there. **Carrie Kirby** ***San Francisco Chronicle*** Right, did you know when? **John Thompson -** ***Symantec Corporation Chairman and CEO*** We ve all been saying this year some time. Actually it s now later than we thought, so it shows you how difficult this challenge is. So the fact that they re going to have something late in the year as opposed to midyear as we had originally forecasted suggests that this is not a problem that s easily solved. **Carrie Kirby, San Francisco Chronicle** Did the prospect of this have anything to do with your decision to diversify Symantec? **John Thompson -** ***Symantec Corporation Chairman and CEO*** Not at all. We had been on a path as a company to be a bigger player in the enterprise security space for a long time, in the enterprise software space for a long time. And so I could care less about what Microsoft does. I m more focused on what our customers needs are and how we can do a better job of serving them. **Curtis Schauger** ***CIBC*** This question is more geared towards the customers up here. It would seem that those models proposed by Symantec, the power of it is addressing diversity, particularly as we think of the battle between Linux and Microsoft and its dominance the server and client landscape. How much value do you put on enabling diversity across your platforms and still maintaining availability and security? And does that balance of power in terms of a vertically integrated vendor offering the entire stack completely, they could make it available, but is there inherent weaknesses of doing that and when does the balance or is the balance going to shift. How do you grow diversity for diversity s sake? **Tom Jones** ***State of California Department of Health and Human Services*** Can I get that one? **Unidentified Speaker** Sure that s fine. **Tom Jones** ***State of California Department of Health and Human Services*** I ll give you a quick in fact, we went through this last March. We re a full-service data service data center, AFPISV (ph), to a lot of customers, and we don t just use Microsoft in our shop. And so, when we are going out and looking at an enterprise tool that had, basically, a central console, it had the ability to take feeds from all of your intrusion systems, your firewalls, your center live (ph), et cetera, be able to integrate or interface to an org management, a threat management system, to be able to ultimately drive work for patch management and deployment it couldn t distinctly just be Microsoft. For us, it wouldn t work. We could SMS for that. We didn t pick SMS, and in fact what we did is we invited actually Symantec which was late in the game because of their acquisitions of On-Technology to participate in a bake-off of tools that were enterprise driven to able to allow (ph) heterogeneous patch management and work and drive work effectively, and w e re talking about anything that we have on any platform. Symantec is always going to be a part of that for sure, but we actually brought in several other vendors that did that and excluded vendors that only did for archaic (ph), and we ended up with a better product I think. It s going to be scalable, and it s going to take us into that 21st century service delivery model that we really need to do. Linux is a part of that, and we see that coming. Microsoft will always be a part of that. New open source that we don t even know about yet will be a part of that. Got mainframe issues, AIX issues, UX issues, Solaris issues we all have that. So, it couldn t be simply a solution that was just targeted using SMS as the baseline for it. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 8

Final Transcript SYMC Symantec at RSA 2005 Conference David Bank - *Wall Street Journal* Steve Bank (ph) with the Wall Street Journal. John, do you think the link between security and availability is the rationale for the Veritas deal, and the panelists here and others seem to buy that argument. The stock market rewarded that as well though, and I think you said that the initial deals would all come back and I think later you said you were surprised, the haircut (ph) you ve taken. **John Thompson *Symantec Corporation Chairman and CEO*** I m not allowed to use those terms anymore. (LAUGHTER) **David Bank *Wall Street Journal*** Are you still surprised? And what is the market missing or what does the market know that you re missing? **John Thompson - *Symantec Corporation Chairman and CEO*** Well, I think that s a better question for this crowd than for me. We are determined to get this done. There is no backing down. This is by far the most profound thing that our company can do to serve the needs of our customers. And so, regardless of how the equity markets respond to the transaction, we re moving ahead because it s the right thing for the technology category that we are part of. Now that being said, most investors have some difficulty dealing with change particularly when the change is as monumental as they perceive this change is and, hence, they respond as they have with Symantec. But in the past when other companies, and we, have made changes in our strategy to address a broader range of opportunities there s been the haircut (ph) as you called it, not me, that has occurred in the equity markets and it has come back, and I firmly believe that that will happen here that as we successfully integrate Veritas into our company, you will see the light and the representation or value of the equity will respond correspondingly. **Tim Klasell *Thomas Weisel Partners*** question for the customers as well. You all, sort of, spoke to the vision of the integrity of the process in how, maybe, Symantec s working (ph) with Veritas may be able to create. Inside of your organization, are you organizing your people like that? Do you think you ll start making purchase decisions around this, or will we still for some time see the security guy and in the data center, the storage and backup guy? **Malcolm Kelly *Reuters Global IT Security Director*** I ll just respond to that. I m responsible for operational security sources within the bigger operations department that provides services. We re actually organizing now to bring that together as part of a risk and control department looking at the whole aspect of risk and control within operations, so that will include power supplies and data sensors and availability issues across the whole spectrum. So we re certainly bringing it all together. **Rich Baich *ChoicePoint Chief Information Security Officer*** If I could add to it, I mean we re not talking about anything new. This is business continuity planning. So if it comes down to how as an organization approaching security in my particular organization I also had DRBCP, so I welcome the opportunity to operate and, kind of, focus the efforts around that much more because if not. I had another whole organization that I have to go across to go through collaboration to get it done. So I think this will actually help put it availabiltiy as part of the purchase process of some organizations where it may not already be. **Unidentified Speaker Richard Jackson *ChevronTexaco Chief Information Protection Officer*** I d like to address that also. We are also integrating our information risk components into a single entity, and the strategy is to try to influence the procurement process. I think it s critical because typically when you re out procuring products and services, the focus is on functionality, performance, and security becomes an afterthought. So we re going to try to inject risk into the selection process early on. ***Jon Oltsik Enterprise Strategy Group Senior Analyst, Information Security*** The gentlemen from the Wall Street Journal asked before about that action. As I said before, I talked to full constituencies. Usually, this is not a big surprise. This does make intuitive sense, and even, say, companies with functional barriers of, say, a networking group, a storage group, a security group they re still working vertically on business processes so it s an application environment, business process, it s reducing business risk. So they re looking at Symantec and saying okay I get it, but let me see what happens versus the Wall Street guys who are acting very tactically may not understand all the Veritas products, may not understand all the Symantec products. So, what you re hearing from the users is really, kind of, everyday logic in their world. **Garrett Bekker *Tradition Asiel Securities***

Sort of falling under the same theme that last question, basically, what I was trying to get it I was wondering, maybe, if there have been any changes in the purchasing decision that are made, the way you view purchasing decisions from either the security or storage **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 9

Final Transcript SYMC Symantec at RSA 2005 Conference side, if there is any change, what has been driving that? Is it compliance? **Rich Baich** ***ChoicePoint Chief Information Security Officer*** I ll take, I guess, first digs at that. It comes down to business continuity planning. I think it s being driven by customers, partners, and potentially future regulations that organizations have to ensure that they have a survivability plan in place. It s one of the most difficult things to do in an organization, and the market is maturing. The customers are getting I won t say smarter but more demanding. As a result of that, you re seeing much more, I should say, service level agreements, and consequently organizations now I can speak to my own as well as colleagues I ve talked to out there they re putting security as part of the acquisition process and actually I can take it a little bit further. Post 9-11 commission has been, I think, an amendment to (inaudible) The Clinger-Cohen Act in the government which actually requires information security to be part of all acquisitions. So, I think in general people have recognized the importance, but it s a change in process that has to happen. **Tom Jones** ***State of California Department of Health and Human Services*** One of the things that I ve noticed is that there s a lot of uncertainty right now in how you spend your dollars. In the government, obviously, they have to do more with less. Everybody s familiar with California State government issues, but one of the things that is very difficult for us is some of the maturing that Richard just talked about is creating confusion on how to spend your dollars wisely because you re seeing, for example, a convergence of a lot of functionality either into that - maybe you already have solutions for and you don t want to duplicate. In other words, you want to really be able to buy right. You want to buy properly integrated systems, or if you re going to walk away from technology make sure that you ve got the right kind of replacement technology and there s a lot of evaluations that are going on, and frankly some of the vendors are actually doing some market control by announcing stuff that s really vaporware (ph) right now. And I m not going to mention anybody, but that s a problem for us because if you re already kind of connected with one vendor and you re looking this way, and there s a product coming, you might have a tendency not to buy and then you ve got risk because you ve got vulnerability you can t protect against. So from our perspective, its very, very an issue, it s a huge issue on how we buy. **Richard Jackson** ***ChevronTexaco Chief Information Protection Officer*** Our processes are being driven by, I think, three factors Business Process Enablement, which is indicative of the recognition of having certain process in place, you need to have risk understood and managed. Second issue is compliance. A lot of the regulations are beginning to impact us in a significant fashion and we have to actually comply with all of those laws and regulations. But clearly, there s costs because if they don t do it right the first time, eventually I find out about it and they ve got to redo it over again, and that s a cost factor and we can t afford to pay duplicate costs. **Joe Menn The LA Times** Hi. This is for Mr. Thomson and I apologize for harping on this as somebody said we ve seen some of these movies before. You re doing a lot more with spyware, anti-spyware products there were just press releases so apparently is Microsoft. Your s aren t free. There s is. You re not a monopoly, they are. Has there been any... **John Thompson -** ***Symantec Corporation Chairman and CEO*** I wish I was. (LAUGHTER) **Joe Menn The LA Times** ... any internal consideration of pointing out any anti-trust issues to the EU... **John Thompson -** ***Symantec Corporation Chairman and CEO*** I d rather fight Microsoft in the marketplace because we re convinced we can whip them. So this is not about showing up in Washington or whining on someone s doorstep about what Microsoft can or might do. To the extent that they violate the position of prominence that they have, we ll be watching, but whining in Washington about press releases or pointing to left field by Bill and his team, I mean, of what value is that? **Riva Richmond** ***Dow Jones*** Reva from Bajon. This is a follow-up actually, this question. Since Microsoft is going to offer some level of viral protection for free **John Thompson -** ***Symantec Corporation Chairman and CEO*** You get what you pay for. Remember that. **Riva Richmond** ***Dow Jones*** Well, what s that going to do to the spyware market at least for the consumer? For the panel, to what degree does that begin to address this issue for you, or is it not enough? **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 10

Final Transcript SYMC Symantec at RSA 2005 Conference John Thompson - *Symantec Corporation Chairman and CEO* I ll defer to the customers. **Tom Jones** *State of California Department of Health and Human Services* I told you yesterday I was just trying to build a Valentine s Card for a friend of mine and I did nothing innocuous, and I had two active real time pest spyware agents running and another one that we re all familiar with Ad-Aware running, and all I did was to right-click copies and I told you that you know if it could happen to me behind my firewall, behind my protection systems knowing full well what I m doing imagine what is happening every single day to consumers. Obviously, we re jabbed about the possibility of getting integrated spyware prevention. I ve been trying to find out where Symantec and CA and everybody else is going in terms of their real time protection because that s where I think the real value is. This after-the-fact scanning, that s cool. I ve been scanning my machines for over a year using these SpyBot and Ad-Aware tools every night, and I continually find stuff everyday and I don t go to sites that are problematic. I simply went to Google search for Turkish Angora, American Standard, and Pento Max right-mouse click each of those and put them onto a card, said Happy Valentine s Day, sent it off, looked at my machine - 179 critical objects. This is a problem, okay, so we ve got to get some solutions. I know we don t want to talk about packaging in terms of tools but it is a lot of people would say, wow this is really cool and it is real cool, but one of the tools that I had up running was Microsoft s basically anti-spyware beta one. It didn t get the things that it said it should have gotten, okay. **Rich Baich *ChoicePoint Chief Information Security Officer*** I just want to make sure one thing. I know 9-0 Enterprise (ph) has anti-spyware in it, and I think 10-0 (ph) is going to have an industrial (ph) grade, so I m confused that the next Symantec includes it in their product for free. **John Thompson - *Symantec Corporation Chairman and CEO*** Our view of the market has gotten good. The spyware market has a temporal financial value. In other words, there s a moment in time when certain portions of the market will, in fact, be willing to pay incrementally for advanced protection and removal capability. And since we are a for-profit software company, it is our intent to look for the opportunity to seize on that temporal moment in time. However, as time moves on, it s clear that large enterprise buyers, for sure, and to a lesser extent in the early timeframe, consumers and small business owners will not be willing to pay for that level of capability. They will expect that to be dealt with in malicious (ph) or Malware detection. So our strategy has been to incorporate detection capability, and spyware detection capability has always or not always but certainly in the current version of the NAV product has been there what we re doing in the Almagen release, which is the internal code name, is giving you advanced detection capability and removal capability for a broader range of threats. It s in there. It s not about going now and saying you ve got to pay me a little bit more. Admittedly, if there s a sales person out there that won t try to get a little bit more for it, I want to know his or her name. **Jeff Englander** *Kaufman Brothers Analyst* Jeff Englander from Kaufman Brothers. The dismissal Carly Fiorina from Hewlett Packard has been - **John Thompson - *Symantec Corporation Chairman and CEO*** What does that have to do with this? (LAUGHTER) **Jeff Englander - *Kaufman Brothers Analyst*** I like the risk of big mergers. Can you differentiate for us this merger and your experience, any lessons you may have learned there? And to the customers, what you would like to see with Veritas (ph) as the merger proceeds forward to avoid any similar mistakes moving forward? **John Thompson - *Symantec Corporation Chairman and CEO*** I can t speak for what HP did, but I can speak for my experience both at IBM and at Symantec. And I ll preface this with saying, Gary Bloom and I in our roles as CEOs have done almost 30 transactions. So it s not like we are novices or neophytes at this notion of acquiring and integrating companies and, more importantly, their people into our organizations. The two things that are critical in every transaction first, the speed of decision making. Make sure that you have issues that are brought forward that are fact-based and you are prepared to make decisions right then. And part of the reason we chose to, this time, unlike all of the other transactions we ve done, we chose to engage outside consultants to help us because it will remove or eliminate some of the emotion from the rendering of facts, hence making decisions a heck of a lot easier. Second point is the broad and repetitive nature of the communications process that has to go

on, and clearly when the organizations are going to amass roughly 6,500 people from one company and 7200 or 7300 from another company, there is an enormous communications task. Not just internally but externally as well. And so, speed of decision making and clarity of communications are the most important things for us to make sure we get done right if we re going to be successful in this process,

Final Transcript SYMC Symantec at RSA 2005 Conference and I am convinced that we will be, independent of what happened at HP; I don t know much about that. **John Thompson -** ***Symantec Corporation Chairman and CEO*** Well take one more and wrap it up. Ok. (PAUSE) Alright, well, look, thank you very much. First, let me thank the customers for sharing their point of view. We value not only their confidence in our company but their willingness to speak out about their view of how the industry will evolve, and I appreciate your interest in what we re doing and how we re going to make Symantec a success. Thank you very much. **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. **Thomson StreetEvents** streetevents@thomson.com 617.603.7900 www.streetevents.com 12