VERITAS SOFTWARE CORP /DE/
Form 425
February 18, 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

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 speech given by John Thompson, Chairman and Chief Executive Officer of Symantec Corporation, at the Empire Club on February 17, 2005 and has been posted to a joint website hosted by Symantec and VERITAS.

Bowdens Media Monitoring Limited

BOWDENS RADIO/TV TORONTO
Tel: 416-750-2220 Fax: 416-750-3250

John Thompson Empire Club Thursday, February 17, 2005
(Transcript)

PODIUM (ROG-TV), TORONTO, 17 Feb 05 REACH:174,000, 13:00, Length: 00:43:00, Ref# 4518ED-1

JOHN W. THOMPSON

JOHN W. THOMPSON, HOST: Thank you very much, Bart, for that very gracious introduction, and good afternoon everyone. It s clearly a pleasure to be with you here in Toronto and have an opportunity to speak to such a prestigious audience. It s my understanding that the club dates back more than 100 years, and as a part of that process it s also my understanding that the speeches that are given here are, in fact, published and provided in a year book to secondary schools, to universities, to elementary schools throughout Canada.

Now when I heard about that I thought gees what an honour, quite an honour. And I started to think about my ten year old granddaughter and whether or not she would even pay attention to what I have to say today, (laughter) much less something that might be in the archives 100 years from now. And so it truly is an honour and hopefully an opportunity for me to suggest to my granddaughter that there are people who will pay attention to at least one thing that I say.

As Chairman and CEO of Symantec I m often called upon to talk about what s going on in the Internet and what the trends are that are affecting the IT industry. And so what I d like to do is spend some time with you this afternoon sharing with you what I share with colleagues and friends as well as government officials and regulators around the world about the trends that we see emerging in information technology.

My being invited to speak here today, I think, demonstrates the growing interest and importance of IT and the fact that it s no longer an isolated area of responsibility. As a matter of fact the area of IT that we are focused on, information security, has clearly now become a boardroom issue. Now because of that we, as an industry, need to move away from some of the jargon that we use and so our world needs to be eliminated of some of the many acronyms, IDS, and UDBM, and AV and all of those things so that you can get to the simple essence of what we do, which is all about protecting the vital infrastructure and information that you rely on to make business decisions, and maybe even personal decisions every day.

What we need to do is to make sure that, that infrastructure, when put in place, can recover from an incident very quickly, and more importantly you have the confidence in which to make appropriate decisions about running your business. And so our job at Symantec is to make sure that the applications that you use for business decision-making are allowed to stay up and running no matter what might happen.

As you might imagine my opportunity to speak with audiences carries me to parts of the world near and far. But there s one thing that is common about every place in the world, and that is our customers are dealing with three very, very vexing challenges and they re consistent around the world: cost, complexity and compliance.

Now cost is one that is certainly not a new nemesis to the IT domain, it s something that we ve had to deal with for quite some time. As a matter of fact hardware costs have come down quite substantially over the last few years, but the real challenge for many IT organizations has been the labour cost associated with running and managing their environments. And as more systems and applications are being deployed, as more security vulnerabilities are discovered every day and as their the number of users required to be served by this infrastructure grows there s no question that, that cost is challenging.

The next big challenge is complexity. Your IT departments have traditionally had to deal with the complexity of the computing environment and tried to make it transparent to many of you. They re also managing the ongoing challenge of integrating disparate operating environment, operating environments from windows, from Solaris or Unix in a range of operating systems. This is an enormous amount of complexity and it is getting greater, not less, in its difficulty.

Today the Windows environment is still the most exploitive from a security point of view but other platforms, including Linux, are now demonstrating similar weaknesses. And it s this level of platform growth that ensures that there will be a tax on those new environments as well. And it is in that vein that we at Symantec certainly applaud what Microsoft is doing from the point of view of its security initiatives. We also recognize that what they are doing is necessary, but not necessarily sufficient, for what every large enterprise user must have. Large enterprise users have a requirement for multi-platform or cross platform in the vernacular heterogeneity and therefore it may be impossible for someone who is so focused on one environment to genetically move to support others. That s why Symantec and other purpose-built companies will in fact, we believe, be a better alternative for security than someone who is so focused on one particular environment. And we re also mindful that we re not distracted by things like computer games, and things that don t relate to securing your infrastructure.

Compliance is also the new elephant in the room and it s one that we certainly have to be mindful of. You can t avoid bumping into some new regulatory requirement today. Regulatory requirements around retention of records, the discovery and retrieval of information, audible processes that can in fact determine whether or not your business is

running appropriately, and clearly security breach disclosure is a paramount issue.

In Canada you re grappling yourselves with a number of regulatory initiatives like PIPEDA or PIPEDA, depending upon your choice of explanations. And in the U.S. clearly we are struggling with Sarbanes-Oxley. If you are in one or another vertical industry around North America there are no more than one or two regulatory initiatives per industry that you must conform to, and it s in that context that this new elephant in the living room is one that we have to deal with.

Compliance has become a top priority for CEOs around the world and it certainly is wielding considerable influence over IT budgets and IT decisions and it s no exaggeration to suggest to you that it will in fact be the challenge of the 21st Century.

So in this evermore complex, more costly, more regulated environment, it s no wonder that many of you want a more integrated solution to manage your infrastructure and you d rather work with a strategic partner who can help you do just that.

Now don t get me wrong I m not suggesting that you re going to buy all of your IT solutions from one vendor, that s highly unlikely. But I m also not naïve enough to think that we can t provide more than we do today. So the drive to deal with the vexing challenges of cost complexity and compliance, are in my opinion, going to be factors in consolidation in our industry over the course of the next few years. I would predict that our marketplace is going to see fewer vendors, better product integration, improve inoperability and fewer complicated license agreements for all of you to negotiate. In other words fewer hoops and hurdles for all of our customers around the world.

At the end of the day what that suggests that only a few of us will be able to deal with the growing challenges that you face, and it s my belief that those who are global in nature and well prepared will be able to handle that challenge as well.

Now one of the things about the security domain that is real is that we know that the motive of the attackers is changing. From the notoriety amongst a small group of friends to today geopolitical power and in many instances financial gain. At Symantec we identify about 100 new viruses every week and we see about 48 new software vulnerabilities every week, and that vulnerability represents the gap between when someone discovers something and when it gets attacked. Once upon a time that gap represented six months. Today that gap is less than six days. Last March, the Witty worm attacked a vulnerability that had only been disclosed 24 hours before that. And we are clearly on the cusp of what we call day zero attacks where the vulnerability and the exploit occur almost simultaneously.

As we are all well aware cyber threats go well beyond malicious activity around worms and viruses. Today spam, spyware, phishing, identity theft and fraud represent the new face of cyber crime. Spam is turning out to be more than the great nuisance. I think Canada s own Federal Industry Minister, David Emerson, described it best when he said and I quote, A few years ago spam was a mild irritant, today it s become the cancer of

the e-economy. Spam has become one of the most severe threats to individuals in businesses and today it s suggested that it represents more than 66% of all e-mail traffic.

Phishing, which is spam s evil stepchild, is growing at an alarming rate. From September to October of last year the number of phishing sites, hence the opportunity to steal someone s identity or information that could be used of value, doubled in one month. Disguising themselves as well- known, highly reputable institutions like CitiBank or eBay, phishers con unsuspecting consumers into volunteering personal information. In fact their hit rate is 5%. Now that s five times greater than any physical catalogue campaign that a mass marketer would institute.

Now while the consumer is certainly a victim of this fraud perhaps the greater victim is the banks, the retailers or the government institutions whose brands have been unwittingly compromised and hijacked. Businesses must fight back against scams to protect consumers but also to protect themselves and their brands.

Finally businesses in government offices need to be prepared for both natural and manmade disasters so that, that infrastructure that they are relying on can in fact carry the vital information for their industry. Even something as common as a server failure can have a serious impact on productivity and the profitability of a particular business.

Our own research suggests to us that it costs ten times as much to recover from a single incident or a disruption than it does to prevent it on the front-end. Our information is at risk, ladies and gentlemen, and the risk mounts with each and every passing day, as does the value of the information that s being targeted. Information is in fact the lifeblood of almost every organization today and it s worth more than the individual piece parts that store it, manage it or retrieve it or distribute it, combined. Yet we rely on information to serve customers, doctors rely on information to render diagnosis for patients and utility companies rely on information to distribute energy. So, today, we truly do live in an information-based economy where data is not only the important currency as was suggested by Bart, it increasingly is in fact the product itself. And that product is under increasing attack and I d like to share with you a simple story of how that is occurring around the world.

Unleashed in January 25th, 2003, just a little over two years ago, the Slammer Worm exploited a vulnerability in Windows- based operating environments that had been identified six months earlier. Slammer was aptly named. It slammed the Windows systems rendering them inoperable, doubling its infection rate every eight and a half seconds. It was the first of the so-called Warhol worms, a reference to Andy Warhol s famous quip about everyone having fifteen minutes of fame. In Slammer s case it was ten minutes. It infected 90% of the unprotected servers in just ten minutes worldwide. Airline flights were cancelled; ATM networks stopped working; whole businesses went down.

As soon as the word got out that Slammer was in the wild the mad dash began to quickly identify vulnerable IT systems and patch them and to make critical backup data sets available. Once Slammer hit, companies

struggled to bring their businesses back on line. As a matter of fact in some instances it literally took days. It was clear that companies didn t know enough about their IT infrastructure of their environments to take immediate action. They didn t have the necessary processes in place to recover from such a disaster. In the end, the damage exceeded $1 billion worldwide, according to Computer Economics. That s just the clean-up costs, that doesn t even begin to account for loss productivity or loss revenue, or more importantly loss customer trust or customer confidence. So an event like Slammer has a major ripple around the world. Indeed Slammer impacted the global economy in a way that no other single attack ever had and it didn t even carry what we in the
trade call a malicious payload.

So what are the lessons that we learned from Slammer? What did Slammer teach us about protecting the information assets that are so critical to our economy? Well we learned that our view of security was far too narrow. We learned that we had to focus more on not just protecting the device or the network but our focus needed to be more on the information itself. Once the dust settled on slammer customers made it clear that we had to serve them differently. We had to protect their information differently. We had to make sure that it was not only secure but that it was available as well. Information that is available but not secure, may very well be useless. It s like putting your information in a safe, or your valuables in a safe, and then forgetting the combination all together.

Our goal is to strike the right balance between making information secure and making information generally available. Symantec has been helping customers solve this problem for quite a few years from our simple beginning and the largest segment of the security industry called content security to the introduction of our first integrated security appliances about three years ago. Our integrated security solutions have helped many of you, I believe, take cost and complexity out of managing your security environment. Now we think we need to look beyond cost and complexity to deal with the issues of compliance as well. And today we argue that it s more about an integrated infrastructure approach not just an integrated security approach. It s about seamlessly bridging the divide and that s an important phrase, bridging the divide, between device management, systems management and network management across a disparate operating environment, because security as traditionally defined is no longer good enough. We re in a different game with different rules and far, far more stringent requirements.

Slammer showed us that even when we as security professionals, did everything right, alerted our customers to the impending threat, updated signatures and definitions, and recommended a response, it just wasn t adequate. Traditional security wasn t then enough and today even integrated appliances fall short of some of the requirements that our customers have. They couldn t ensure that their business would stay up and running no matter what, therefore new proactive technologies incorporated into the concept of an integrated security appliance will in fact help prevent some attacks but then the question becomes one of recovery.

Our researchers have been hard at work to stay ahead of the attackers and making the process of security far less costly and far less complex. But we must shift our game to offence, where we are driving the overall process of protecting critical information, not

just responding to known threats or visible attacks. In other words we must take an approach to this far more proactive and far more holistic in dealing with the issues before information is compromised, stolen, affected or misused.

After Slammer we realized that to be a strategic partner to our customers we really had to take a more bold step. We had to connect external threat information that we have in our laboratories with internal knowledge that customers have about their operating environments. While an external early warning system is clearly a valuable asset and a valuable head start, if you can view into the horizon, it doesn t necessarily save all of your assets. It would be like a hurricane brewing on the horizon where you know from the radar that it s on its way and you know that it s going to hit within a few hours. That s good to know short of being able to get plywood and duct tape and all of the necessary precautions to board up your windows. Now imagine, however, if the radar tracking a hurricane s progress could talk to your home, could in fact trigger the automatic activation of your hurricane shutters and the automatic activation of sump pumps.

To truly protect assets, we need to be able to act on external threat information and have that talk to the IT infrastructure and have it drive process and change. So let me have you imagine with me a scenario. What if an external threat could alert and trigger an internal audit? You could instantly identify the systems that might be available or vulnerable to an attack. Take it a step further. What if the external alert could tell systems to patch processes or applications in those vulnerable systems and automatically update those that are unprotected? What if external intelligence could prompt more frequent backups to critical data from an end-user device all the way up to the largest data centre our mainframe environment? What if the early warning system could trigger the automatic fail over to a secure network environment and prompt the restoration to a trusted state once the threat level had passed? And what if all those actions could produce an audit trail to ensure your policies and processes were conforming to internal or external compliance requirements?

Now we would argue, and I think you would agree, that would be pretty useful. However, that might be challenging to implement. And so the question for Symantec after our analysis of the Slammer attack is: how do we start to work towards delivering that level critical infrastructure protection? After Slammer we realized that we needed to strengthen our portfolio in areas of asset management and storage management so that we could deliver that kind of solution to you around the world. By combining the unparallel capability that we have in security intelligence with the capability to understand what systems environments customers were wanting, that would be an important step forward in critical infrastructure protection.

So we made two simple acquisitions of a little company called PowerQuest and one called ON Technology. These were not security companies and many said I don t understand that. They specialized in data recovery, in client and server provisioning, in inventory and asset tracking, in software distribution and patch management, all critical items for managing the IT environment, but they re not security technologies. At that point we could offer both security and availability solutions with one small caveat, we

could only do it in a Windows environment. And there is, to the best of my knowledge, no, certainly few, large enterprises that are Windows only. So to serve the needs of customers we certainly needed to have a far more comprehensive portfolio.

And it was out of that simple concept of how do we serve the needs of customers better that our merger with VERITAS was born. Pure and simple: it marries the market leader in security technologies with the market leader in storage and availability management. And it gives us depth of capability across every single platform being deployed by a large enterprise customer around the world. The new Symantec following the merger with VERITAS will serve the full spectrum of customers, from consumers to the largest government and commercial users around the world. We will operate at all tiers of the IT infrastructure and on virtually every single platform.

So let s take a look at an area where we think wonderful synergies between these two might come into play. Compliance is about understanding risk and developing strategies to mitigate risk. The compliance process requires protection and remediation technologies coupled with policy management solutions.

Symantec has many tools and services that can help information technology teams navigate their way through the growing thicket to ensure regulatory compliance, but an integrated solution also requires capability to ensure that the data is maintained and it is available at the data centre level all the way down to the individual PC level.

It also requires cataloguing and indexing of capabilities for discovery and retrieval. In some industries today the storage and retrieval of e-mail messages is almost as important as the banking or financial information about the company. Sure you could cobble all of these together with various vendors but getting them from one might certainly make the process simpler and less complex.

Looking at the information security needs through the eyes of a business executive today it s clear that there are heavy demands weighing on your agenda, all requiring immediate action. You need to reduce the risk of managing your information. You re worried about security and privacy and the availability of the data itself. You want to shield the information you safeguard from threats and you need to prove to regulators that you can produce accurate, auditable records upon demand. And as security and availability converges it s my strong sense that your security teams will focus more on managing and mitigating risks as opposed to blocking attacks.

Already we are seeing the emergence of risk management groups with a far more over arching responsibility for information management across the entire enterprise. It s in this space that we believe that there will be a redefinition of roles, a redefinition of the role of what security is performed and how security is managed across the large enterprise. No longer will we be the custodians of information security, we are the stewards, I believe, of the integrated infrastructure challenged with making them both more secure and more available.

The annals of commerce are filled with examples of companies who have transformed their model and in doing so transformed their industry. Perhaps a classic example that I m familiar with is from the package delivery business. In 1998 UPS embarked on a transformation that was, as its CEO, Mike Eskew, described as radical as any it had done in its 97 year history. They no longer wanted to describe themselves as just being in the package delivery business. No longer were they responsible for the pick-up and delivery of small packages. As a matter of fact they viewed that they were in the global logistics and supply chain management business. Its new charter was to enable global commerce, the flow of goods, information and funds all on an international scale.

Today, UPS acts as the fulfillment centre for Nike.com; it s the repair centre for Toshiba laptops; it even recycles many of the old discarded PCs that many of you may have gotten rid of.

I would argue that we re at a very similar juncture in the information security industry s life cycle. We are at the cusp of an enormous opportunity on the frontier for information technology. Our paradigm has shifted. Until today we chartered this frontier of the IT environment as security specialists. We patrolled its borders, we spotted threats and we alerted those at risk. It s time for us to do more. It s time for us to do more than raise red flags and block threats.

Integrated infrastructure management means addressing all forms of risk before they strike as well as after. It s about disaster recovery. It s about systems availability. It s about proactive protection of the entire infrastructure, especially the information. In the old paradigm we were only as good as the last update. In the new paradigm sensors will prevent attacks. And when it can t alerts will trigger a patch distribution and provisioning and backups so information stays secure and available, and information technologists stay focused on innovating instead of fighting fires.

In a world where our most vital and valuable asset, information roams the Internet, where network walls no longer exist, where the threats to information are rampant and accelerating. The regulatory demands for security and privacy are incessant. We need to move beyond a security only focus and stake out our place, I argue, in the information management category. But these are only the first steps in an ongoing journey. There s still more that we can do expanding our role to managing systems availability, network access and performance of applications must be a part of that critical mission. In the end, helping our customers manage and protect the content that rides over the Internet.

Leaders never follow and innovators see opportunities often where others don t. Fortune always favours the bold. Those who take proactive and comprehensive approaches to ensuring the integrity of the information and the resilience of the infrastructure in the future will, in fact, be the winners in the IT game. To get real value out of the information assets we truly must protect them. We must balance the needs of availability with the imperative for security, and we need to expand beyond the traditional borders if we want to effectively address both of those needs. At Symantec we intend to lead, we intend to innovate, and we intend to be first movers so that we can, in fact, continue to be your trusted advisor.

I thank you so much for the opportunity to be a part of the Empire Club s event today and I thank you even more for your support and trust and confidence in our company. Thank you very much.

[Applause]

END