SYMANTEC CORP
Form 425
March 01, 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 communication contains forward-looking statements, including statements regarding industry trends, such as supplier consolidation and growth in security attacks, benefits of the proposed merger involving Symantec Corporation and VERITAS Software Corporation, such as improved customer and platform coverage, improved product capabilities and lowered customer costs, post-closing integration of the businesses and product lines of Symantec and VERITAS, future stock prices, future product releases and other matters that involve known and unknown risks, uncertainties and other factors that may cause actual results, levels of activity, performance or achievements to differ materially from results expressed or implied by the statements in this communication. Such risk factors include, among others, deviations in actual industry trends from current expectations, uncertainties as to the timing of the merger, approval of the transaction by the stockholders of the companies, the satisfaction of closing conditions to the transaction, including the receipt of regulatory approvals, difficulties encountered in integrating merged businesses and product lines, whether certain market segments grow as anticipated, the competitive environment in the software industry and competitive responses to the proposed merger, and whether the companies can successfully develop new products and the degree to which these gain market acceptance.

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

Additional Information and Where to Find It

Symantec Corporation has filed a registration statement on Form S-4 containing a preliminary joint proxy statement/prospectus in connection with the merger transaction involving Symantec and VERITAS with the SEC on February 11, 2005. Any offer of securities will only be made pursuant to a definitive joint proxy statement/prospectus. Investors and security holders are urged to read this filing (as well as the definitive joint proxy statement/prospectus when it becomes available) because it contains important information about the merger transaction. Investors and security holders may obtain free copies of these documents and other documents filed with the SEC at the SEC s web site at www.sec.gov. In addition, investors and security holders may obtain free copies of the documents filed with the SEC by Symantec by contacting Symantec Investor Relations at 408-517-8239. Investors and security holders may obtain free copies of the documents filed with the SEC by VERITAS by contacting VERITAS Investor Relations at 650-527-4523.

Symantec, VERITAS and their respective directors and executive officers may be deemed to be participants in the solicitation of proxies from the stockholders of Symantec and VERITAS in connection with the merger transaction. Information regarding the special interests of these directors and executive officers in the merger transaction is included in the preliminary joint proxy statement/prospectus of Symantec and VERITAS described above. Additional information regarding the directors and executive officers of Symantec is also included in Symantec s proxy statement for its 2004 Annual Meeting of Stockholders, which was filed with the SEC on July 30, 2004. Additional information regarding the directors and executive officers of VERITAS is also included in VERITAS proxy statement for its 2004 Annual Meeting of Stockholders, which was filed with the SEC on July 21, 2004. These documents are available free of charge at the SEC s web site at www.sec.gov and from Investor Relations at Symantec and VERITAS as described

above.

The following is a communication and a link to an article that was sent by Symantec on February 21, 2005.

THE WORLD ACCORDING TO **JOHN THOMPSON**

Gatekeeper to the world of business

Early warning is vital to security Symantec s chief tells **Karen Dearne** at the RSA information security conference in San Francisco

IT s a marriage of heavyweights. Internet security provider Symantec will soon tie the knot with enterprise software maker Veritas in a $US13.5 billion ($17.2 billion) merger.

For Symantec chairman and chief executive John Thompson, the deal is more than just another step in Symantec s transformation from consumer antivirus software publisher to global leader in information security products.

Thompson is following his hunch that large enterprises are ready to talk to a single vendor offering integrated security and system management products across mixed environments.

For it s no longer a Windows world, he says, and even Linux networks are under attack.

Is it true you ve got a team out the back knocking out viruses 24 hours a day?

We have a team of guys who are defending the network from virus attacks 24 hours a day. They are global in their mission. We have a research lab in Australia, we have one in Tokyo, one in Santa Monica and one in Britain.

Given the nature of the threats out there, it s impossible to do it in a consolidated or centralised way, so having a distributed research function is an important part of helping to protect customer networks.

There s a lot changing, for you and the industry. Your latest acquisition, of Veritas, seems to signal your intention of providing a full line of security services.

Well, it s our belief security technologies are necessary but not sufficient to deal with today s attacks.

What s happening is that vulnerabilities are being exploited, and if you can use early warning and intelligence about potential exploits, or potential attacks, you can do things on the infrastructure side to mitigate the risks such as reconfiguring a server, doing a real-time back-up or reprovisioning an application in such a way that it s less vulnerable than it might have been.

Tying up the domains of security, systems management, network management and storage management is the only way you re going to create a truly resilient infrastructure that can prevent attacks or recover quickly when an attack occurs.

What s the thinking behind this integration strategy?

After we did a post-mortem of the Slammer attack of January 2003, it was our belief that, given the fact that customers had had a six-month warning of the vulnerability in the Windows Server environment, and they had not done anything, we needed to do more on the management side, not just on the protection side, to help ward off such attacks.

So in late 2003 we announced the acquisition of PowerQuest and ON Technology, which gave us Windows-based provisioning capability for back-up, recovery and patch management for software distribution for a broad range of

things to manage the Windows infrastructure.

We concluded, after integrating those functions, that we had many of the components to help mitigate risk in the Windows environment, but there s no large enterprise that s Windows only.

Many of them have Unix-based systems, they have Linux-based systems, and a growing array of mobile devices, and so we needed broader platform coverage and that s why Veritas is becoming part of our family.

We now have broad-based coverage at every tier of the infrastructure, and on almost every platform that is part of the infrastructure.

JOHN THOMPSON ON
Attacks

Tying the domains of security, systems management, network management and storage management is the only way to create a truly resilient infrastructure that can prevent attacks, or recover quickly when an attack occurs.

Recovery
Helping customers recover from an attack is almost as important as preventing the attack, because it s inevitable networks are going to be attacked, it s inevitable the data stored there is going to be compromised.

Branding
There s only one company, and that is Symantec. There s no debate about that. It is one of the most trusted brands as well.

Is that where you see your future strength?

If you think about the way attacks are occurring, about half the attacks on the network are in the Windows environment and the other half are not Windows-related.

They re in other operating environments that customers in large enterprises have deployed.

If we re going to be effective in helping them secure and manage such infrastructure, we have to have coverage of those other platform environments as well.

While preventing attacks is a critical part of what we do, helping customers recover from an attack is almost as important as preventing the attack itself, because it s inevitable that networks are going to be attacked, and it s inevitable that the data that s stored there is going to be compromised in some way.

So, how do you help restore the environment to a state that s more trusted, to an environmental condition that you know is resilient and ready for real-time? That s our focus as a company.

Are you re talking about situations where you know an attack is coming so you stop the system and take a snapshot of it before it hits?

Yes, you might take a snapshot of a server, so you know the configuration of the server, and you know the vulnerability, so you push a patch, that will block the attack that may be the subject of that particular vulnerability.

Or, you know there s an attack ravaging the internet, so rather than doing the daily, weekly or monthly back-up, you back up straight away, because if you do it immediately, if the system does get compromised, the recovery is a lot faster because the spot you have to recover to is more recent than it would have been in your normal back-up schedule.

The whole security paradigm has evolved from being solely about technologies for detection and prevention to a process that needs to be deployed for understanding the assets on the network, understanding attacks and vulnerabilities, and linking your knowledge of these to provisioning and protection capabilities.

If we do that as we have planned, we think we can deliver something that is uniquely relevant to the problems of today.

So this approach is aimed squarely at enterprises?

It s a large enterprise play. It s not about the consumer per se, although you could in fact, through what we do with service providers, do more to make consumers better protected. A lot of the insights we have about security threats to the extent that we can re-plumb a service provider s infrastructure based on our knowledge would help consumers and small businesses served by those providers.

There s a lot of different security hardware and software products out there. Are people confused about the choices they have to make?

Just the sheer fact that there are thousands of exhibitors here at the RSA Conference suggests there s a complexity customers have to deal with that is growing every day.

I m not trying to say the world s going to move to a one-stop shopping place.

What I am trying to say, however, is that the combination of cost, complexity and the growing issues around compliance in the IT environment will drive customers to want to do more things with fewer vendors. It s going to drive customers to the point where they want to see better interoperability between products; it s going to drive customers to the point where they ll decide they d rather bet their infrastructure s resiliency on a well-established global player that can help deal with through the myriad choices out there.

That lends itself well to industry leaders like Symantec, frankly.

Microsoft is putting a lot of effort into improving the security of its products. Will that cut across your market share?

If you consider what everyone is speculating about Microsoft entering the security domain with a range of technologies there s no large enterprise in the world that s Windows only.

So Microsoft is probably genetically incapable of serving the needs of a large enterprise because they don t do anything other than Windows.

There s an enormous void that needs to be filled where we can have common capabilities spanning not only the Windows multi-tier environment but the environments of HP-UX, of AIX, of Solaris, a range of other proprietary platforms and the growing Linux world, which is becoming one of the top-of-mind issues for CIOs.

Do people see a problem with Microsoft checking its own security homework?

I ll let the market decide that. I think if I were Microsoft, I would stay focused on building a stronger, more resilient operating system, and leave the responsibility for protecting the applications and data to purpose-built companies like Symantec, but I m not going to tell Steve Ballmer and Bill Gates how to run their company either.

Veritas is strong in storage, archiving and systems management, areas that are necessities under the new regulatory regimes that are emerging.

Correct. It s our belief that the new elephant in the room that everybody has to deal with is compliance, whether it is the horizontal layer such as Sarbanes-Oxley and certification in the US, or the vertical compliance that each industry has to deal with.

Compliance is driving what CIOs and business leaders are doing to ensure the integrity of the information that s in their infrastructure.

The focus on compliance lends itself well to a broader portfolio, because you not only want security technologies to block attacks or threats, but you want compliance technologies to ensure you are meeting the auditable standards for your industry, or your conformance to the IT policies that you have in place.

Hence, the compliance capabilities that Veritas has, coupled with the compliance capabilities that we have, over time will offer a compelling solution to customers.

How will you bring the two brands together?

There s one brand, and that brand is Symantec. We will integrate the technologies, but we will preserve the market brands that are associated with the products.

So Net Backup or Backup Exec and KVS, which are products in the marketplace, will retain their known identity because buyers have an affiliation with the brand.

There s only one company, though, and its name is Symantec. There s no debate about that.

It s interesting, because you have a very high brand profile with regular users, as well as business users.

Well the combination of Symantec and Norton has been around now for almost 25 years, and it continues to be one of the best recognised brands in the industry.

Quite frankly, around the security and management paradigm that customers are dealing with, it is one of the most trusted brands as well.

It s on the basis of that trust that we know we have to do more to help customers protect their environments, and that s why the Veritas transaction is so important in our quest to fulfil a broader mission for customers and a broader mission, quite frankly, for the industry overall.

Are you planning to drop the consumer side of the business?

Not at all. Our consumer business is a powerful part of our portfolio.

It s my belief that the profile of the high-performing software company in future will be one that not only has a well-established presence in the enterprise, but one that has a well-established presence in the consumer and small-business markets as well.

Few software companies in the industry look like Symantec today. Post-Veritas we will have 25 per cent of our revenues coming from the consumer business, and about 75 per cent of our revenues coming from small businesses to large enterprises.

It s a very, very powerful combination and one that allows us intelligence and insight that is not readily available to companies that only focus on one buyer segment.

What are you seeing in terms of new threats?

Well, the new threats are certainly more frequent, more complex and spread more rapidly. That s what has led to our belief that security alone is necessary, but not sufficient.

We are expanding our portfolio to use intelligence and early warning insights to drive a range of systems infrastructure retooling to make sure we can ward off an attack, or recover from an attack very quickly.

If we do what we plan, we think it will propel the growth of our company for many, many years.

If you take a look at our Deep Site alerting service, Deep Site tracks known vulnerabilities or new discoveries around the world. We literally have the capability to track more than 3000 products from roughly 1900 to 2000 vendors around the world.

We literally have tens of thousands of sensors deployed to track intelligence about network attacks. We have 140 million to 150 million consumers and businesses out there feeding us intelligence every day about what s going on with their networks.

So the question is, can we harvest all of that information to deliver real-time alerts that drive customers through automated actions to reconfigure their environments to do more pro-active security, as opposed to reactive security measures?

Are you talking to government about this?

Absolutely. Government organisations represent probably 15 or more per cent of our enterprise software revenue.

In the US Department of Defence, and in most of the defence agencies around the world, Symantec has a very strong presence.

What about organised crime involvement in network attacks today, and the commercially targeted attacks that are occurring?

It s clear to us that the motive for attacks is changing, and therefore the attackers are changing.

It used to be a small group of friends who were doing it for notoriety. Now, it s more for geopolitical power reasons or for financial gain.

That changing motive suggests to us that the value of the information to be protected has certainly gone up, and therefore we have to be more thoughtful about the security process.

It s no longer about an intrusion sensor, or a firewall, or antivirus software.

Those are important but they are only components in a broad security scheme.

The more progressive organisations, such as those in financial services, recognise that security is a process that is augmented by technology, but it s not the technology itself.

Is it an advantage for banks, for example, to tell customers that their network is secured by Symantec, because that s a brand they recognise?

We have some relationships with banks where they will say: Powered by Symantec or Protected by Symantec . Typically they want to use our brand when they want to go to their customers, because customers recognise the awareness and visibility of our brand at that level.

So there are a couple of institutions in the US, in Canada and in Europe, that offer a Symantec provided service to their customers as they come into the bank s infrastructure.

It goes beyond banks to all sorts of e-commerce scenarios. Consumers are still sitting outside, thinking they don t want to do business online because it s not safe.

That s an issue that the whole industry certainly needs to be mindful of.

If consumers and small businesses, in particular, lose confidence in their ability to transact simple things over the web, or to facilitate commerce between themselves and their partners or customers over the web, that wouldn t be good for the IT industry.

I don t want to take on the mantra that we re going to protect the world, but I think we do need to be mindful that if the erosion of confidence about online transactions continues to grow, that s not good.

What can the industry do about that?

Education and awareness are very important, and we ve been on that campaign for a number of years.

We were a founding member of the Cyber Security Industry Alliance, which helps to get the message out to government organisations around the world, because government in every country has a role to play in raising the awareness of the simple things individuals and companies can do to protect themselves in a wired world.

Through industry collaboration with governments around the world, we can raise awareness and that will dispel some of the fear that may be settling in, but it s going to be a long-term effort.

It s not something that s going to happen overnight, for sure.