VERITAS SOFTWARE CORP /DE/
Form 425
April 21, 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 article 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 (Symantec) and VERITAS Software Corporation (VERITAS), 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 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 article. 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, 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 article. 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.

The following article by Dave Clarke Mora entitled C.I.O., Redefined Information without integrity isn t enough was posted on Symantec s intranet on April 20, 2005.

Upload VERITAS **Executive Briefing** Volume 1, Number 2 2005 Tools, tips, and strategies for information executives

C.I.O., Redefined

Information without integrity isn t enough.

By Dave Clarke Mora

There must be something in the clear, Kansas air that breeds confidence. Renowned adventurer and aviatrix, Amelia Earhart, hailed from Atchison. In the film classic, *The Wizard of Oz*, Kansas farm girl-turned-tornado-traveler stands up, undaunted by any wicked witch crossing her path. And in a field northeast of Wichita, John W. Thompson learned a thing or two about fearlessness from, of all things, a few wild turkeys.

Chief integrity officer

Thompson, chairman and CEO of Symantec, the world s leading provider of cyber security software and solutions, knows a thing or two about boldness. He was appointed by President Bush to sit on the United States National Infrastructure Advisory Committee to provide counsel on securing the nation s IT infrastructure. He was tapped to chair Silicon Valley s Blue Ribbon Task Force on Aviation Security and Technology. And, in newspapers and magazines, and on billboards around the world, Symantec s ads offer not just odes to the fearless, but declare that you too, should Be fearless.

It s an audacious assertion in a world where CIOs face a nonstop barrage of cyber threats, ever-evolving system vulnerabilities, and increasing demands on their resources from government regulators and market pressures. It s a bold statement, Thompson acknowledges with a broad smile. But it s about the

John W. Thompson, Chairman and CEO, Symantec

simple idea that someone who is not concerned about the information being compromised, who is not concerned about making information too broadly available, who has the right controls and procedures around information dissemination, can be fearless about access to systems. It says, Be prepared to open your electronic doors. Be prepared to give unlimited access to your information to those who have to have it, because you have the right security and availability strategy around those assets. So be fearless.

C.I.O., Redefined

Underpinning that pluck is the principle of information integrity, something Symantec builds into each of its offerings from the ground up. Information integrity, Thompson says, is about striking a balance between having information readily available to anyone who needs it for decision making yet having that information secured so that it cannot be compromised or lead to an incorrect decision.

And it was that notion, that in order for information to be valid and valuable it must be secure and available, that helped spur the dialogue between Thompson and another highly regarded high-tech CEO, Gary Bloom of VERITAS, which ultimately led to the companies announcing their intention to merge in December 2004. That marriage between security and availability can be very powerful for large enterprises, Thompson says.

The power of one

The intent to provide CIOs with powerful tools that help them leverage and protect their existing technology investments so they in turn deliver value to IT and the enterprise at large has shaped Symantec s product development strategy since Thompson took the helm there in 1999 after nearly 28 years at IBM.

One of the unique things about being Symantec, about being in the security business, is that customers can see the cause and effect between our product and the performance of their infrastructure, Thompson explains. For example, with LiveUpdate, a tool we innovated that automatically downloads protection updates against security threats in real time, CIOs know that every day we deliver a new piece of technology to help protect them in one way or another. And they know that were it not for that piece of software, an attack could bring down a significant portion of their infrastructure.

But it s not just the cause and effect between implementation and protection that has driven CIOs to favor Symantec solutions. For several years now, the company has worked toward providing an integrated product set. We ve broadened our portfolio compared to other security software or technology companies, Thompson explains. Our strategy has been about product integration. That s our secret sauce. What does integration do? It takes out complexity. What does complexity reduction do? It reduces cost. The relationship between price

That marriage between security and availability can be very powerful for large enterprises. ***John W. Thompson, Chairman and CEO, Symantec***

and value, price paid and value received, is clearly apparent to them. CIOs can really say, These guys are, in fact, focused on driving value for us.

The strategy seems to be paying off for Symantec s shareholders and customers. The company s revenues increased by more than 30 percent for fiscal years 2003 and 2004. In a 2003 *CIO Insight* survey, Symantec ranked highest in overall value among some of its most critical constituents, CIOs and IT executives at enterprises large and small. In 2004, the company placed second behind Red Hat.

We ve been able to demonstrate, time and time again, that you can reduce complexity and therefore, operational costs, by doing more with one supplier, says Thompson. That s borne out, he believes, by the increasing number of large transactions Symantec is engaging in with customers where multiple products are part of the purchase. And, If integrated security was important, we think integrated infrastructure will become even more important. That s tying security and availability together the way we planned it.

Between a rock and a SarbOx

New compliance regulations, and the fervor with which they re being enforced, are helping CIOs and other senior information executives get the message to C-suite executives that attention must be paid and resources allocated to ensure the reliability, integrity, and availability of the IT infrastructure, according to Thompson. Sarbanes-Oxley and other overarching regulatory initiatives are forcing the C-level to become more attuned to the operational risks in their IT infrastructure. Consequently, they want to know more about the risks to that infrastructure. They want to know how to mitigate those risks with policies and procedures that are auditable, that can be inspected, and assure resilience and compliance to company policy or industry requirements. Now, when executives have to sign on the dotted line to affirm the accuracy of their financial statements and filings, says Thompson, increasingly, they re more inclined to be concerned with the integrity of the information their data enables, and who has access to it.

Chief Integrity Officer
John W. Thompson

Title: Chairman and CEO, Symantec

Born: Florida, 1949

Education: B.A. in Business, Florida A&M University; M.S. in Management Science, MIT

Family: Married; two children, three grandchildren

Most respected business leaders:
Jack Welch at GE did a terrific job of focusing on executing strategy consistently; John Chambers at Cisco Systems because he is focused on customers and engaged with them every day; Gordon Moore and the succession of CEOs at Intel have done a fabulous job of focusing on their core technology while rendering something as arcane as a computer chip into a commercial hit with Intel Inside.

Given seven carefree days: I d be in Hawaii doing absolutely nothing. I d take a five-to-eight mile walk every morning, come back, take a nice cold shower, get into a hammock, and do nothing.

Favorite meal: Any meal prepared by my wife and me. The process of preparing it is as much fun as eating it.

Favorite tech toy/gadget: The remote control for the TV!

Executive Briefing

John Thompson s Three-point Security Checkup

1. It s important that CIOs step away from the debate about firewalls, or intrusion sensors, or intrusion prevention. Security has to move from being about technology to being about policy and the process around compliance to that policy.

2. Once you understand the security policies

   relevant to your business and your industry, determine what processes you need to implement that policy effectively.

3. With your processes and policies defined, then you can determine which technologies become the instantiation of those processes.

In the security business, time is of the essence. The gap between discovery of a system vulnerability and its exploitation in the cyber world at large has shrunk from four to six months a year or so ago to an average of 6.4 days today. That suggests, says Thompson, that the notion that you will be able to patch for a large enterprise thousands of systems, servers, and desktops has become an administrative challenge that may be unachievable. It requires security providers such as Symantec to be able to block behaviors threatening the infrastructure generically. It means building shields to protect the systems automatically. You have to get ahead of the exploitation component, Thompson explains. That s one of the reasons marrying security and availability is so important. If we see certain patterns emerging on the horizon, we can trigger operational actions in the configuration of the server, the backup and recovery timeframe, or sequencing for the device or application. Those things aren t security related, they re operational. But they reduce the impact of a security breach.

There s dumb fearless and there s smart fearless

For all the talk about intrepid attitudes in business, Thompson says it was a couple of dumb turkeys, and ultimately, his infinitely more intelligent wife, Sandi, who taught him about being fearless. A hunting buddy and I were in a turkey blind in Kansas taking part in the Governor s turkey hunt, he relates. Well, I got one in my sights, took my shot, and killed it. But immediately after, instead of turning tail and running, another male in the flock looking to prove himself the new leader of the pack, decided to stomp all over the one I d shot to prove his machismo. So, I

shot him, too. Witnessing the demise of two competitors, yet another bird stepped over and started stomping on the two I d just shot. So, my hunting buddy shot him. If those three birds had simply followed their instincts to run off, it might have turned out differently for them.

The birds behavior taught Thompson a little about when not to be overly daring. But it was some time later, back home in New York, that Thompson learned the true meaning of fearlessness. After 18 years in a successful marketing career, Thompson s wife decided that she wasn t doing what she wanted to professionally so she quit and went to law school. That was fearless. I saw her do it and realized that if she could do it, so could I. So, after 27 years, 9 months, and 13 days, I packed it in at IBM and accepted the position here at Symantec. Had she not demonstrated what fearlessness is the right kind of fearlessness I might not have made the move.

Had Thompson not made the move, Symantec would undoubtedly be a different company today, perhaps one that doesn t even recognize the importance of information integrity, let alone provide solutions to enable it. But, thanks to three bird brains, one intelligent woman with a passel of gumption, and a man smart enough to recognize the difference, Symantec does. And so, Thompson is right. When it comes to your data and the infrastructure supporting it, go ahead. Be fearless. Smart fearless, that is.

Dave Clarke Mora is editor in chief of VERITAS Upload.

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 Software Corporation. We urge investors and security holders 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. Symantec, VERITAS and their directors and executive officers may be deemed to be participants in the solicitation of proxies from stockholders in connection with the merger. Information regarding the special interests of these directors and executive officers in the merger is included in the preliminary joint proxy statement/prospectus described above. Additional information regarding the directors and executive officers of Symantec or VERITAS 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 or VERITAS proxy statement for its 2004 Annual Meeting of Stockholders, which was filed with the SEC on July 21, 2004. Investors and security holders may obtain free copies of the documents described above and other documents filed with the SEC at www.sec.gov or by contacting Symantec Investor Relations at 408-517-8239 or VERITAS Investor Relations at 650-527-4523.