REMARKS BY JOHN W.THOMPSON
STORAGE NETWORKING WORLD; PHOENIX, AZ
APRIL 13, 2005

BREAKING DOWN THE BARRIERS: BUILDING THE RESILIENT INFRASTRUCTURE

Thank you for that kind introduction, and for welcoming me to Storage Networking World.

It's an honor to be here, although let's be honest: some of you are surprised to see me, the CEO of Symantec – a company many of you associate solely with security software -- here at a storage industry conference.

Yet, in many ways, being here today is a homecoming for me. Thirty-some years ago I was a rookie storage sales rep for IBM in Atlanta, Georgia.

I'll never forget the first time I walked into a data center. The mainframes were humming. The disk drives were running like crazy. It was an amazing sight.

And I walked up to this disk drive, and I pulled this plug out, looked at it, and put it back in.

Almost instantly, I heard the operator yell, "Oh – and I can't repeat the word here! What the hell happened?"

It turns out that plug was a magnetic signal that had the address for the drive. When I pulled the plug, I – this rookie salesman walking into his first data center -- crashed the whole system.

I guess you could say that I learned very early on the types of security threats to data – since I was one.

Back then the crown jewel of our product offering was the 3330 Model 11; it had the awesome storage capacity of…200 megabytes. And that capacity came at a price…with a purchase price of about $80,000, the price per megabyte worked out to about $400. Now, of course, the price per megabyte is less than one cent.

But the cost of storage is not all that has changed over time. Back then, while information was important, it tended to be payroll or supply chain-related. Back then, companies ran costly fault tolerant systems for mission-critical applications.

The world is very different today. Business requires that storage be dynamic, on-demand, and tied to almost every piece of the IT infrastructure. And, most of all, information is what creates value for your organizations.

Information is **the** currency of our age, and as such, it has become invaluable. Unlike a disk, a server, or a laptop – it isn't replaceable. That's why your job is equally invaluable – because every organization needs to ensure that their information -- the data that travels through their IT systems – remains protected…recoverable…and manageable…every minute of the day.

It's been amazing to live through the ups and downs of our industry over the last 25 years. And, lately, I have found myself returning to my roots. A little over a year ago, Symantec expanded its business to include systems management, back-up and recovery, and patch management capabilities.

And, in case you haven't heard, we are in the process of merging with VERITAS.

However, what brings me here is not nostalgia, but a clear-eyed view about the future – the future of security…the future of availability…and how they must be intertwined if we are to better leverage information to help companies grow into new markets and new services.

In the years ahead, there will be few challenges greater than protecting and efficiently managing information. It is nothing less than the lifeblood of your organizations…even our global economy.

So, today, I'd like to spend my time with you talking about the challenges we as IT professionals face and some of the possibilities for addressing them.

I want to discuss how re-thinking the way enterprise IT works can help make the infrastructure more agile and more resilient.

I want to explore how changing how IT runs can enable companies to bounce back from disruption and optimize performance…and most of all, free you to do what you're meant to do: think creatively, innovate constantly, and push the boundaries of what's possible.

And the people on the frontlines of this transformation – those who will be asked to do more to add value – is all of you. You are at the vanguard. You will make this change happen. So, it is truly exciting to be here with you at this conference.

(PAUSE)

Of course, protecting information isn't without challenges – challenges all too familiar to those of us with years of experience in the industry. These include: cost, complexity, and risk management.

The first challenge is one every enterprise IT department faces: controlling costs.

I don't need to tell you the pressure that IT departments are under – you live it every day. But the most recent CIO Insight survey really paints the picture. It found that almost two-thirds of CIO's surveyed weren't facing flat IT budgets…they were, in fact, facing shrinking IT budgets.

Hardware and software costs keep dropping, but the operational costs to manage the infrastructure have continued to increase. At the same time, the volume of data is exploding – growing at an average rate of 60 percent per year.

That means you have to find ways to do your day-to-day job with less money, fewer people, and fewer overall resources. That means finding ways to standardize as much as possible and be more productive in managing your environment.

And -- oh -- by the way, you must do all of this while working on new projects, such as building applications that will provide strategic value to your companies.

(PAUSE)

But that's just the tip of the iceberg.

There's also the increasing complexity that comes with managing the flow of information across your business.

Right now, you have Solaris running on some systems. Windows running on others. Not to mention a host of other proprietary platforms. Plus, Linux has appeared as the low-cost alternative.

You have desktops…laptops…PDAs…wired…and wireless networks. In addition, you're managing any number of hardware and software combinations. Not to mention different versions of software. All of this only adds to the complexity of your environment.

(PAUSE)

But as they say on TV…if that's not enough…we'll throw in risk management.

The third challenge you face is one that recently has increased in scope, and that's managing risk. That includes everything from security threats…to business continuity…to compliance.

Today, there are any number of threats to information – acts of God…errors made by people who have approved access to your networks…and attacks launched by those who don't. And, of course, there's the rookie salesman – or CEO – who thinks he can walk into data centers and pull random cables out of machines.

Seriously, let's not kid ourselves…outside attacks are increasing in number, in frequency, and in sophistication.

The most recent Symantec Internet Security Threat Report released last month – the most comprehensive gauge of the Internet threat landscape -- found that malicious code that exposed confidential information made up 54 percent of the top attacks in the past six months -- that's up 10 percent from the first half of last year.

Symantec documented about 1,400 new vulnerabilities, or 58 new vulnerabilities a week. The majority of these gaps in programming code had moderate or high severity, and almost half of them occurred on Web applications.

Not only are the number of vulnerabilities growing, we're also seeing exploits appear at a faster pace. The average span of time between the discovery of a vulnerability and it being exploited has collapsed from six months… to six days.

Last March, for example, the Witty worm attacked a vulnerability that was discovered just the day before. "Day-zero" attacks are just around the corner. In other words, we'll soon see a vulnerability and an exploit attempt will appear on the same day… almost simultaneously!

Of course, internal events such as systems failures or human error, can also impact business continuity. Yet many enterprises don't have adequate disaster recovery plans in place. Or, if they do have one…they haven't tested it. They don't know if back-ups are created…if they can replicate to another site…or seamlessly failover to another server.

(PAUSE)

Yet, cyber threats, system failures, and natural disasters are not the only source of risk. Increasingly, public companies have a compliance risk that they must contend with – from Sarbanes-Oxley to other regulatory demands such as G-L-B-A…
HIPAA *[HIP-ah]*...PIPEDA *[PI-PE-DA]*…and Basel 2.

The truth is that you just can't avoid bumping up against some new rule or regulation and its information-related requirements – whether it's records retention…discovery and retrieval…auditable processes…or security breach disclosure.

(PAUSE)

Trying to do more with less…managing an increasingly complex and heterogeneous environment…all the while reducing risk is a pretty large task.

It calls for a flexible, agile foundation to run and store critical information…while protecting it from a number of risks.

And it demands a broader view of how to integrate security and availability.

This point was driven home to me on January 25, 2003 – the day Slammer hit. As many of you know, Slammer was a worm that exploited a vulnerability in Windows-based servers that had been identified more than six months earlier.

Slammer was appropriately named. It slammed Windows systems, making them inoperable. Slammer doubled its infection rate every 8.5 seconds…and within 10 minutes, it managed to cripple more than 90 percent of vulnerable systems.

Slammer flooded networks all over the world. Airline flights were cancelled. ATM networks stopped working. Whole businesses shut down.

In the end, the clean-up costs alone reached $1 billion worldwide – and the cost in terms of lost revenue, productivity, and customer confidence was several times that.

It was clear that companies didn't know enough about their own internal environment to take immediate action.

They couldn't proactively manage their IT environment. They could see what was coming, but they didn't have the tools in place to avoid a disruption. They struggled to quickly identify vulnerable IT assets…patch those systems…and back up mission critical data.

As a result, once Slammer hit, companies struggled to bring their systems back online. In some cases, it took days. Many didn't have the necessary procedures in place to recover quickly.

Now, the thing to remember about Slammer is that it didn't have a malicious payload – meaning, it didn't alter or delete critical data. It could have been worse.

But what Slammer did to was open our eyes to what could happen if such an attack or other type of disruption did occur.

It drove home the fact that we needed to be more proactive in how we manage the IT infrastructure and handle the vulnerabilities and threats to it.

(PAUSE)

Slammer was a wake-up call for our customers. In fact, it should have been a wake-up call for the entire IT industry. And if Slammer wasn't enough, the blackout of 2003 should have been another eye-opener.

No longer could security be divorced from storage and systems management. To get the most out of our information, it had to be secure and available.

After all, information that is secure, but unavailable is useless. It's like putting all of your valuables in a safe… and forgetting the combination. And, information that is widely available, but not secure, is worthless. It's like putting all your trade secrets up on a billboard.

That's why enterprises need to create a foundation that ensures that their information is trustworthy and reliable. They need to know that their information has integrity.

We need to take a more holistic view of information management. That way we can prevent an attack… quickly recover in the event of a disruption…and make day-to-day operations run more smoothly.

That means creating a resilient infrastructure that is flexible enough to respond to an ever-changing IT environment, but rigid enough to withstand an attack or disruption.

It means building a solid foundation that can seamlessly bridge the divide – and that's an important phrase – bridge the divide between security…device management…storage management…and systems and network management.

That way you can find the right balance between risks and costs…optimize the flow of information through your organization…and, preserve the availability of key systems.

(PAUSE)

How could this convergence help you mitigate risks and protect business services? How could marrying external insight about threats with internal intelligence about the IT environment help you avert or weather an approaching threat…without interrupting your business?

I grew up on the east coast of Florida, so the idea of a hurricane warning system comes to mind. You can see the big storm brewing on radar and you may know when it's going to hit. But, what can you reasonably do – besides scrambling to buy plywood and duct tape?

Now, imagine that the radar tracking the hurricane's progress could "talk" to your home directly and trigger the automatic activation of hurricane shutters and basement sump pumps.

That would be pretty cool, wouldn't it?

When a threat is on the horizon, you need to be able to act on external intelligence immediately… which means that your security system needs to be able to "talk" to your information management capabilities… directly... and, on an ongoing basis.

Picture this scenario.

What if an external threat alert could trigger an internal audit? You could instantly identify the systems most vulnerable to the attack.

Take it a step further. What if the external alert could tell systems to assess patch levels on those vulnerable systems and automatically update those that were unprotected?

What if that external intelligence could prompt more frequent, incremental backups…in an end-to-end fashion from user systems all the way through to the data center?

What if that early warning could trigger an automatic "fail over" to a secure network? And, prompt the restoration to a trusted "clean state," when the threat passed?

And, what if all these actions could produce an audit trail to ensure that your policies and processes are in compliance?

That's what we envision when we talk about a resilient infrastructure: the integration of external and internal insight, of security and availability.

That's what we picture when we talk about implementing end-to-end solutions that can proactively protect and recover IT assets…maximize data and application availability…and, preserve business continuity.

(PAUSE)

But that's just one part of having a resilient infrastructure. It's also about optimizing the performance of your applications and systems.

It's about being able to measure performance in an end-to-end manner and ensure optimal service levels for every segment of your business.

It's about improving day-to-day operations.

Take e-mail management. It's probably one of the biggest and most important tasks that we all face.

You must be able to store, manage, protect, and recover e-mail. If not…if it goes down, so does productivity. After all, for most people in corporate America, e-mail going down means taking a two-hour lunch.

In an infrastructure that balances security and availability, you would see the threats coming and be able to take proactive steps to block them. You'd be able to filter out the spam and other garbage so your network and servers are free to process the mail you want…and, by doing that, you would free up your storage capacity for the data you need to run your business.

You'd have the ability to recovery lost e-mail and archive it to meet regulatory requirements. And be able to catalogue and index it for easy discovery and retrieval.

With a resilient infrastructure in place, "neither rain nor hail…nor sleet nor snow…nor heat of day nor dark of night" will stop the e-mail or other mission-critical applications from working. They will be there when you need them. And I say that as the son of a postman.

Sure, you could go out and piece together this solution from various vendors. But, it would only make your IT environment more complex, cost more money, and make it more difficult to mitigate your risks.

(PAUSE)

Every transformation needs a leader…someone who sees the possibilities before others do. Someone to take that first bold step.

After all, throughout the history of business, change usually comes from one company leading the way. Think of the automated assembly line: the concept was around for a few years, but it took Henry Ford to put it into practice and revolutionize manufacturing.

It was a bold step, but one that had to be taken.

In our own time and industry, Symantec intends to be the one to lead the way.

We've listened to our customers, and they were clear…they want a partner to help them protect their information – no matter what they are using to run it. They need solutions that work on the variety of systems– across all platforms.

It was out of this desire to fulfill customer needs that the merger with VERITAS was born. It marries the market leaders in both security and storage.

The new Symantec, following the merger with VERITAS, will serve the full spectrum of customers – from consumers to small and mid-sized businesses to enterprises and government agencies of all sizes. We will operate at all tiers of the IT infrastructure -- and on virtually every platform.

We will be uniquely positioned to help you reduce cost, complexity, and manage business risk.

With no hardware agenda, the combined company will enable you to protect your investments in both infrastructure and people. A common set of tools…with a common language working on a common platform…will allow you to shop for hardware as if it's a commodity.

It will enable you to easily transition people to new hardware…without having to train and re-train them as your organization grows.

The new Symantec will be looking out at the world – gathering the information you need on emerging threats and vulnerabilities.

And we'll help you look into your operations -- providing insight into the health of your IT infrastructure. What are your storage utilization rates? What are the availability of your systems and applications in the face of a disruption? And are your back-ups working and is your data recoverable? We want to help you answer these questions.

Combining this insight will help you build the resilient infrastructure that you need…to keep your business up, running and growing…no matter what happens.

(PAUSE)

The combined company will be able to lead this change because we'll continue to change…constantly innovating so we can provide solutions that enable you to focus on innovating in your own companies.

Here are some of the things we have in mind.

Imagine for a moment a world in which back-ups are not just frequent, but are continuous – kind of like TiVO not for your television, but for your data center. Where you can set policies that automate back-ups at the file level or even at the block level…so that when Darlene in HR changes the name of a file or a single word of a document, the back-up happens immediately.

Gone are the all-nighters or the weekends spent backing up data so that you didn't slow the network down during business hours. And, just as you can rewind TiVO when you miss the start of your favorite program…you can rewind your back-up to the precise moment before the disruption -- and bring everyone back online.

And as the back-ups are continuous, the replication to a fail-over site will also occur simultaneously. Backup and replication will become seamless.

Or, imagine an automated system for end-user recovery of data. Instead of Bernie in accounting calling you when he loses a spreadsheet, he will have a Google-like search page…right there on his desktop. He can type in the file name and find a list of all versions that were backed up…and retrieve it instantly. Without a call to IT.

Just imagine a time when you will be able to deliver IT as a measurable service -- aligned with business needs and capable of automatically adapting to change.

By being able to see across the entire information infrastructure, you will be able to ensure that data and applications are always available -- and that performance is maintained at agreed-upon levels. Automated processes will solve problems before they become crises, and most of all, costs will come down as efficiency rises.

(PAUSE)

Ultimately, what we are seeing is a revolution in enterprise IT. And I believe that this revolution will change the job of IT professionals as we know it.

As we build this resilient infrastructure, you will be able to spend less time fire-fighting and more time leveraging IT in new ways to help give your companies an edge. You will be able to focus on creating new ways to boost efficiency and the bottom line -- instead of chasing problems that seem to crop up day-in and day-out.

In a world where the walls between security and operations are no more…in which external intelligence and internal insight about threats and capabilities are seamlessly interwoven…and in which the IT department is focused on delivering a resilient infrastructure, this new focus becomes possible.

This revolution will enable companies to better serve their customers with interfaces that are more reliable and usable.

This transformation will enable enterprises to reap the full benefits of these new technologies.

And, finally, this restructuring will enable you to spend less time with Bernie from accounting troubleshooting his problems.

As a result, it will free you so that you can spend time developing new applications and stretching the boundaries of your imagination and the technology in hand.

It will free you to think strategically and creatively about how to leverage IT to add value to the overall enterprise.

But, most important, it will empower you to align IT to the changing needs of your business.

Stepping back, that is why so many of us got into this field in the first place: because we believe that technology can enable all of us to do what we do more effectively and more efficiently.

Because we see each innovation not as an end – an achievement to be celebrated – but as a step in the process of discovery and progress.

(PAUSE)

And, my friends, while this industry has come along way from the days of tape drives and five-inch floppies…while each day, new ideas are making their way from your white boards to our computer screens…we've only just begun the journey.

We've only just begun to re-focus our work on resiliency and agility… on balancing availability and security…and ensuring the integrity of our information.

We have only just begun to test ourselves and the limits of our imaginations.

We have only just begun to experience the change that will come to our field.

And we have just begun to see the transformations that new technology will make on our businesses and our lives.

It's a new world. We at Symantec eagerly embrace it. And I know you will too.

Thank you very much for your time, and enjoy the rest of the conference.

###

Additional Information About the Merger 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 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.