Today’s Business Imperative: Ensuring Customer Confidence
John W. Thompson
Chairman and CEO, Symantec Corporation
RSA 2007 Speech – As Prepared
February 6, 2007

Thank you for that kind introduction.

This is the third time I’ve had the pleasure of speaking at the RSA Conference. It’s an honor to be here with you this morning and to be part of such an impressive line-up of industry leaders.

Now, let me say right up front that I don’t have any fancy product demos – although we have some great new products like Norton Internet Security 2007.

And I’m not going to spend the next 30 minutes trying to sell you on Symantec or Norton Internet Security 2007 – although I’d love to do that.

No, what I want to do today is to step back from what’s going on in our company and talk about where our industry is today – and where it’s going.

After that, if you want to see a product demo, stop by our booth – and we’ll blow your socks off with our demonstration of Norton Internet Security 2007.

One thing I’ve noticed over the years is that it’s hard to spot change while it’s happening – especially in the information technology business. But since we met last year the online world has evolved.

Take just three popular and very visible examples.

In just one year, the novelty of downloadable, portable music has been replaced with the novelty of downloadable, portable video.

YouTube shaped our politics this past election year just as blogs did in 2004.

And teenagers are just as likely to hang out with their friends on MySpace and Friendster as they are at the local mall.

When you look back over the past year the way we work, play, shop, and communicate has undergone a transformation unprecedented in its scope and speed.

Some say we’re living in the Digital Decade. Others call it the Information Age or the Any Era. Whatever we want to call it, we’re living in an era of more collaboration and online interactions…an era in which the user is in charge. It’s no wonder that *Time* magazine’s Person of the Year for 2006 was “you.”

This change is showing up in unexpected ways. A few weeks ago, I read about a new phenomenon called "BlackBerry orphans" – kids who complain that they have to compete with mom and dad's BlackBerrys or Treos for attention. Their parents are busy reading email during soccer practice, dance recitals, and even while driving carpool.

Imagine that.

Of course, no one would ever think of doing that during a keynote speech at the RSA Conference – right?

Seriously, the advancements we've seen recently have profoundly changed life for the individual consumer – and for the enterprises serving them. In a relatively short amount of time, the entire online world is touching our lives in very different ways than we expected just a few short years ago. Today we're more influenced by connectivity and more dependent on digital content than we ever thought possible.

Think about how you shop. Until recently our shopping was more local than global. We used to go down to the local market to get essentials. Today those same essentials can be bought online at specialty stores.

Transactions that were once done by a company's employees – from money transfers to subscription renewals – are now done by the customers connecting directly to corporate networks. Today self-service is the norm. People are connecting from a wide range of devices, across wireline and wireless networks, and doing so 24 hours a day.

As a result, the ability to collaborate online, work remotely, and engage in more multi-party transactions has created a whole new set of business models.

What used to be clear lines separating enterprises and consumers have now become blurred as networks are extended to not only suppliers and partners, but also to customers.

In such a world, a few things become very clear very quickly: one, IT systems are not a frill; rather they are essential drivers of collaboration, innovation, and growth.

Two, we've realized that confidence is critical to making all of this work.

Confidence is the essential component if we want to realize the full potential of this connected world.

A few decades ago, confidence came from face-to-face interactions. You trusted the quality of the products because you could see them or test them before you paid for them. You had confidence in your bank because odds were that its officers lived in your community or sat beside you in church. And you had confidence that an urgent request for money was legitimate because it came directly from someone you knew.

Now, at a time when the whole world is connected, it’s harder to have that same degree of confidence.

How do you know what is being sold to you on an auction site is what the seller claims it is – and how does the auction site validate the auctioneers?

How do you make sure that when you are logging on to your bank that it’s actually your bank and not a dummy site?

How do you know that the confidential information about your business that now resides with a supplier or a vendor is safe and secure?

Right now, for many, it’s hard to be confident about any of these questions. And that’s the challenge facing us today – because only by instilling confidence in the connected world can we realize its full potential.

It is the single-most important mission our industry faces. It is the one thing upon which the growth of the online world depends. And, it’s what I want to spend my time talking about this morning.

During the past year, we’ve seen some critical changes in the evolution of security. Today, the battleground for security isn’t just the device. It’s also about protecting the information that is being shared and the interactions that are happening online.

Today, the network perimeter can’t be locked down. It’s no longer defined by physical assets in the data center or desktops in the office. The reality is: people are the new perimeter.

They are connecting to networks through a variety of devices – laptops, desktops, and mobile devices. All of which need to be managed and protected.

That’s why last week we announced our intent to acquire Altiris – because we believe the most secure endpoint is a well-managed endpoint.

With information technology so central to daily commerce and daily life, businesses today need to integrate security from the beginning and develop an end-to-end security approach.

Maybe that’s why over the past few years we’ve seen industry leaders from Microsoft, Oracle, IBM, EMC, and Cisco on stage here at RSA. They finally have awakened to the reality of what you and I have known for many years – security is an essential element of today’s business.

Understanding these changes is critical to us as an industry – and for you as security professionals.

Confidence in the connected world will only come if and when the infrastructure, the information, and the interactions are protected and secure.

Doing that requires that we step back and recognize how critical IT is to every aspect of the organizations we serve…to focus not just on IT security, but to broaden our view to include a vision of IT risk management.

To set this new course towards a risk-based approach, the role of security officers needs to evolve from one that focuses on security to one that is more focused on risk management and its leverage on a company's bottom line.

But before I continue, let me explain what I mean when I talk about IT risk management.

Simply, I mean a process of identifying, measuring, and developing strategies for balancing IT risks and returns.

Of course, this includes the security risks that we are all familiar with – such as external attacks, network vulnerabilities, and protecting the endpoints. But a comprehensive IT risk management program also looks at risks to the availability of data, overall business performance, and compliance with legal and regulatory demands.

This new approach is a natural evolution as IT becomes even more central to an enterprise's day-to-day business and long-term success.

After all, the risks to our business become far more significant as we rely more on the technology infrastructure.

Our research shows that roughly two-thirds of organizations feel that they might be impacted by a regulatory breach and a major information loss every five years. And, 60 percent expect more than one major IT incident every single year.

According to the Computer Security Institute and the FBI, in 2006, the average cost of each incident of unauthorized access to information was $85,000. And each hour of system downtime costs companies tens of thousands of dollars.

And those numbers don't take into account damage to reputation, brand, or any costs of regulatory or legal action.

We also know that these incidents have a measurable impact on confidence – and when that is lacking, it has a big effect on a company's relationship with its customers.

For instance, online retailing continues to grow by leaps and bounds. This past holiday season, consumers spent almost $22 billion at U.S. online stores – a 26 percent increase from 2005.

Yet according to a November Gartner press release, almost $2 billion didn't get spent online last year because people were concerned about security and chose to curtail their shopping online.

Over the past several years, we have done a valiant job in keeping up with the risks users face – yet the threats and vulnerabilities are constantly evolving.

Consider some of the new threats we've seen recently.

Advances in using word recognition to block spam have caused spammers to introduce image-based spam. As a result, image-based spam now accounts for 35 percent of all spam on the Internet.

And, as digital devices are being used in every aspect of our daily lives, we are seeing malware making its way into systems through MP3 players – and even GPS systems.

Remember that the next time you get lost….you can blame it on the virus in your GPS system.

Even the rising concern with security has introduced its own scams. Three out of the top 10 new security risks are attacks that tell users they have a security threat and tries to dupe them to send money in order to have it "fixed."

Today's business models are built around the efficiencies of the connected world. Think about what it would cost to go back to the brick-and-mortar world. Sending a bill via snail mail costs double what it costs to send it electronically. And similar expenses would creep up if suppliers demanded to be serviced offline, and if organizations no longer allowed employees to work remotely.

I don't believe that we have to accept a future where information breaches are inevitable and unmanageable.

And I don't believe that consumers should have to feel that they are running a risk to do something as basic as their holiday shopping online.

I believe that we can dramatically mitigate these IT risks…build confidence in the connected world…and help businesses improve on the investments they've made in information technology. The question is: how?

To start, organizations need the right technologies.

Antivirus and firewall solutions are a first line of defense. But with new threats, we cannot become complacent and pat ourselves on the back for solving yesterday's problems. We also shouldn't assume that a less vulnerable operating platform delivers adequate security against tomorrow's threats.

Instead, we need to constantly innovate and develop new solutions to keep pace with the evolving risks to enterprises and consumers alike.

There is no doubt in my mind that managing user identities is the most pressing challenge facing the industry today.

At the corporate level, the deployment of identity management systems has essentially stalled. But changes in corporate governance requirements and other regulatory initiatives will force enterprises to restart these projects. Part of that will mean extending identity management beyond the enterprise to the customers, partners, and vendors that they interact with.

We must give consumers ways to protect their identity and to gauge the reputation of the sites they visit.

What I'm talking about here is a user-centric approach – versus a technology- or platform-centric one. After all, the goal is to protect the user – regardless of the device they use, online transaction they undertake, or threat they may face.

That's why last week, at the DEMO technology conference, we unveiled a prototype of the Norton Identity Client, designed to help consumers manage their online identities and secure their online transactions.

This new technology – representing one of the next steps in our Security 2.0 strategy – will help users protect their identity by giving them one-time-use credit card numbers and other ways to interact with sites without disclosing all their personal information.

The solution can help users tell if a site is not legitimate by alerting them if the site's security certificates aren't valid…if it's a phishing risk…or if its business practices have been rated poorly by others who do business with them. With all this information in hand, the consumer then can determine if they want to do business on that Web site.

Protecting identities today requires that we help consumers make smart choices, safeguard their personal information, and provide a portable solution that can be used on any device.

As consumers get access to more information about a site's security and reputation, I believe we'll see a consumer-led revolution.

Consumers will demand that enterprises conform to a set of technologies and business practices. They'll demand a certain level of security before they're willing to connect. So, I encourage each of you to think about what you can do today to help customers that interact with you have greater confidence in your business.

Implementing IT risk management programs requires us to take a broader view of security management. Organizations need to have a comprehensive view of what is happening across the Internet and within their own environment – and to be able to take action in real-time.

That takes piecing together the right technologies to monitor the threat landscape and evaluate one's own security posture, the right policies to know how to react to incidents, and the right personnel to make sure it all runs according to plan.

This all starts with intelligence – knowing what threats are out there. Our Global Intelligence Network, for instance, consists of more than 120 million systems, 40,000 intrusion detection and firewall sensors, and 6,200 monitored and managed security devices worldwide. Combined with our vulnerability database – one of the world's most comprehensive – we can give organizations the deep insight they must have to protect their infrastructure.

Once you have access to intelligence, you need a way to connect it to a technology platform that enables you to understand what's in your infrastructure. That means leveraging technology that collects data from traditional security solutions, such as antivirus, firewall, and intrusion detection products, and network infrastructure devices, operating systems, and databases. Then it's a matter of correlating the data with the external intelligence to prioritize critical incidents within your own network.

It's also critical that a solution enables you to store and archive data related to security events, ensuring that you have an audit trail to help you understand whether or not you are in compliance with internal IT policies and external regulations.

Responding to potential risks also takes the right personnel and processes. Organizations need to train their staff in security best practices, hire people who know how to manage an IT risk management program, and make sure they've put into practice the right procedures.

Whether you manage this internally or partner with a security vendor, the right intelligence and technologies combined with the right people and practices can make the management of IT risk efficient and effective.

But to truly deliver confidence throughout the connected world, it will take security companies and their customers partnering together to deliver user-centric solutions.

The paradigm has shifted when it comes to security. Enterprises now have the responsibility to secure whoever connects to their networks – especially their customers. We have to assume that they are not protected and provide the security that enables them to interact with us safely – and to have confidence in that connected experience.

To help organizations do this, last fall we announced Norton Confidential, a unique online transaction security solution that allows financial institutions to help their customers bank online with confidence.

Accepting responsibility for the security of a device accessing your network – when it's not owned or managed by you – is a radically new concept in our world.

But more and more, vendors will need to deliver solutions that enable organizations to deliver a secure experience to end-users – regardless if they are partners, suppliers, or customers. Those that embrace this approach will not only reduce their risks – but, I believe, they will also create a competitive advantage for their companies.

Looking ahead, we know that building confidence in a connected world won't be easy.

It will take new approaches to how we work…new technologies…and the right people and policies.

It will take looking at security in the context of an entire IT risk management program. If we do that we can reduce costs, increase overall efficiency, and focus more on innovation.

And it will take us, as an industry, banding together and making sure that we have a seat at the policymaking table when it comes to information security issues. We need to speak up when it comes to matters such as data breach and data retention…or on the issue of global consistency in policies and standards such as Common Criteria and IPV6.

That's why organizations like the Cyber Security Industry Alliance are so important at this inflection point in our industry. If you don't know much about them, I encourage you to learn more. And if you haven't joined, please do. They are our voice – and it must be heard.

Finally, building confidence in the connected world is everybody's job. No one company is going to secure everybody. And certainly, no one can do it alone.

No company is so dominant or so all-knowing that it can provide the level of confidence needed throughout the entire online world. That's why we have partnered with Accenture, VeriSign, Yahoo!, Google, Juniper Networks, and Intel to deliver more robust security solutions. We understand that we're all in this together.

But more than that, who would trust one company to do everything for them?

Think about it: you wouldn't want the company that is keeping your books to audit them. By the same logic, you wouldn't want the company that created your company's operating platform…to be the one that is securing it from a wide range of risks.

It's a huge conflict of interest.

So by working together, we can untangle this conflict of interest. More than that, through cooperation and collaboration – and healthy competition – I have no doubt that we can create the confidence our connected world needs.

When consumers know that their identities will be protected -

When they know that they won't be hoodwinked or defrauded –

And when they know that their data will be secure –

They'll do more online. They'll embrace new technologies and whole new ways of living their lives.

When enterprises feel that they can collaborate safely online with their partners and employees all over the world –

When they feel that they can deliver secure interactions to current and new customers –

And when they know that they are complying with internal policies and external regulations and –

They will innovate and grow in ways they never imagined.

Protecting the connected world is a challenge for all of us – one that we must always strive to meet.

And when we do, confidence will be expected…confidence will be demanded…and confidence will be delivered to every citizen in the connected world.

Thank you.