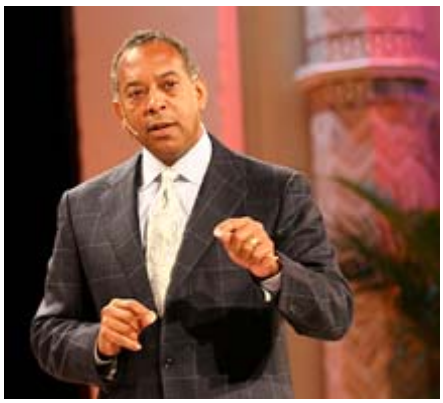
Speaker Transcript

John W. Thompson
Chairman of the Board
and Chief Executive Officer
Symantec Corporation

Keynote at RSA Conference
February 15, 2006

Remarks as Prepared

The growth in online commerce, in broadband usage, and in the number of ways people access the Web has been extraordinary. You don't need to have an iPod, blog all day, or be addicted to your Blackberry to live a digital life.



John W. Thompson explains how the industry needs to evolve to protect digital interactions and give customers confidence online.

Digital interactions are ubiquitous. They touch almost everything we do.

Even when we think we're unplugged, we're not.

Think about it.

Our bills? That handwritten check sets off a digital interaction that zips money out of your account and into another.

Our mail? Scanned and tracked at every step of its journey.

Our groceries? Bought at a supermarket plugged into a global supply chain that can put more cans of tuna on the shelves before we even realize they are gone.

The e-life is here – and changing not only how we live, but what we expect from our lives.

No longer are we concerned about how we are treated by the clerk at the store. Now, we expect instant gratification as we are told our online order has been processed, our shipment consolidated, and items scheduled to arrive in three days.

No longer are there clear lines differentiating business-to-business and business-to-consumer transactions. Now, the two are intertwined – connected by the openness that makes the digital world possible.

And, guess what? Expectations are growing every day.

As consumers, we entrust our family photos, our financial plans, and our e-mail messages to businesses around the world. We trust – and expect – that these companies will protect our personal information as if it were their own.

Think about what consumers are demanding. They want companies to:

- protect their identity, not just their PC;
- to protect their online experience, not just their applications;
- and, to protect their critical digital assets and be able to recover them if something goes wrong.

While customer demands on the enterprise are growing, companies themselves are coming under attack. Firewalls and antivirus software may have kept yesterday's bugs out, but they won't stop an internal data breach, and they won't protect the databases that have become prime targets.

And with each major security breach come new compliance and regulatory demands that are driving expensive technology and operational changes. It's no wonder that more and more enterprises are shifting to a risk-based approach to security.

And that shift can't come too soon. More and more, enterprises are moving to deliver "software as a service" – where the application rests with the enterprise and is just "used" by the customer. With the shift to this model the burden for enterprises to protect customers and their data will be even greater.

Unless each and every one of us – enterprises and consumers - can prove to the other that we are trusted partners, the risks associated with online transactions will become unacceptable.

So, expectations are high. And, the stakes are enormous.

Across industries, companies have built into their business models the efficiencies of these new digital technologies – such as real-time tracking of packages and online commerce.

The continued expansion of the digital lifestyle is already built into almost every company's assumptions for growth – and underpins the assumptions for the global economy.

Think about what would happen if banks were forced to stop all online banking and go back to the days of long lines at teller windows. The costs would be enormous. Today, it costs a bank $10 when a consumer originates a loan online. That cost jumps to more than $200 when the loan is originated through a branch office.

We can't go back to the old way of doing business – and, that's why creating confidence in the digital world is everybody's job.

For an individual company, failure to protect their customers' information will result in customers simply taking their business someplace else, to someone they can trust.

And, they won't necessarily turn to the company around the corner. In the global economy, security can be a competitive advantage – or disadvantage.

If consumers can't trust businesses from our country, they'll look all over the world for ones they believe they can trust. In such a world, security guarantees are very likely to trump the comfort of the local brand.

If we fail to create a trusted digital environment, we won't just slow the growth of e-business, but of all business. We won't just hurt the digital economy, but the economy as a whole.

And, this is the real hidden threat today – not some massive cyber attack, but the loss of consumer confidence in the digital world.

The IT industry has made huge strides these past few years, and from the evidence at hand we've made significant headway in controlling large-scale, fast-moving viruses and worms.

From 2002 to 2004 there were almost 100 medium-to-high risk attacks. Last year, there were only six. The broad adoption of firewall, antivirus, and intrusion-detection software and the progress Microsoft has made in securing its operating platform have made this possible.

Mitigating the virus and worm challenge is a major accomplishment – something to be proud of. But, that's just the low hanging fruit. And, those are yesterday's problems.

Today, we face a bigger challenge.

As you know, sophisticated criminal elements are now behind many of today's attacks – and, unlike the hackers of the past, they are much more interested in anonymity than in notoriety. Today's threats are silent and highly-targeted. What these criminals are searching for is personal and financial information – and they are looking to use it for serious financial gain.

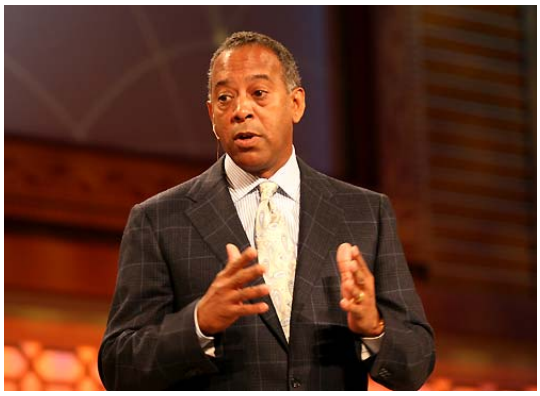
These new attacks really aren't that technically sophisticated. In many cases, they are as simple as the oldest hustles around.

While no one has offered to sell the Brooklyn Bridge online yet, they have tried to sell Mexico, fairy dust, and the meaning of life, which, by the way, sold for three dollars and twenty-six cents.

These socially-engineered attacks take advantage of the naiveté and inexperience of many online users. And, since they are relatively simple, these attacks are easy to replicate.

Consider that every day, as many as 150 million phishing e-mails are launched; and every month 14,000 new approaches are attempted.

Attackers have set up fake Web sites to dupe people into offering up financial information or making a donation to a bogus charity. And, of course, there are large-scale data breaches – some innocent, some inside jobs, and some the work of skilled criminals – that have made identity theft a growing threat to the digital lifestyle.



"If we fail to create a trusted digital environment, we won't just slow the growth of e-business, but of all business. We won't just hurt the digital economy, but the economy as a whole."

For six consecutive years, identity theft has topped the annual list of consumer complaints collected by the Federal Trade Commission.

Last year alone, there were at least 130 large-scale data breaches that exposed more than 55 million Americans to potential identity theft.

The cost of these breaches, in terms of time and money, is astounding.

According to the Federal Trade Commission, identity theft costs businesses $48 billion annually, and last year cost consumers $680 million in losses. On top of that, identity theft victims collectively spent almost 300 million hours trying to repair the damage.

But more damaging than the loss of time and money is the loss of trust in individual businesses and confidence in the digital environment we have created.

Consumers are beginning to hold businesses responsible. And in some cases, they are turning to the courts for protection. Recently, a small-business owner sued a major bank when $90,000 was transferred out of his account after a Trojan attack slipped past his security software.

It's incidents such as this that are causing enterprises to think about the risks they are incurring as they deal with consumers online.

Consumers are also rethinking doing business online.

According to a survey of 10,000 households conducted by the Conference Board, 41 percent are purchasing less online because of security concerns. And, according to a survey by the Cyber Security Industry Alliance, 32 percent of respondents strongly believe that their financial information may get stolen online.

We can't allow trust to continue to erode. We can't continue to lose the public's confidence and expect to continue the robust digital lifestyle that we've come to enjoy.

Trust, ultimately, is the foundation of the online world.

If we – as business leaders – want this digital economy to thrive, it is incumbent upon us to protect all aspects of it – from our enterprise infrastructures to the information created, transmitted, and stored within it. And, most importantly, we must protect the relationships, or digital interactions, that underpin this world.

It's a complex issue – one that won't be solved with a protect-the-PC or secure-the-network mentality. Technology is a critical aspect, but we need to debunk the myth that just securing a network or a device will solve tomorrow's challenges.

We live in a world of all kinds of devices connected to the Internet – PCs, smart phones, and home wireless devices. It's a heterogeneous world full of multiple operating systems, networks, and databases.

So, it would be impossible for any one company narrowly focused only on one aspect of the problem to secure it all.

That's why we must join together as a global business community. To restore confidence, all of us must take responsibility for delivering security to our customers. We need to join together to create a trusted online community. And, we must change public policy so that our customer's most important information is protected.

Don't get me wrong – I'm not saying that consumers don't have a responsibility in all of this. They still need to install security software and should adopt smart online behaviors. But, that will never be enough.

Just as the credit card companies took the risk out of people signing up for credit cards by establishing a $50 liability limit, the business community must offer end-to-end security solutions that take the risk out of the digital world for its customers.

Enterprises should leverage their infrastructures to deliver critical and comprehensive solutions to secure the endpoint and must also protect the applications and databases that hold customer information.

Because let's face the facts: in the digital world, consumers are often the weak link in security. Enterprises are left to wonder if customers are adequately protected. They wonder if their customers could inadvertently expose the enterprise to attack, putting the entire network at risk.

With customers accessing critical business applications, enterprises need a way to ensure that their customers meet some minimum security requirements before connecting to the network.

A solution such as Symantec On-Demand Protection enables enterprises to enforce security policy on guest devices seeking access to the network.

This solution gives enterprises the ability to provide on-the-fly protection to consumers, creating a safe Virtual Desktop environment from which they can interact with the enterprise. The enterprise can even set and enforce connection policies to prevent the export of sensitive company information.

Endpoint solutions give the consumer confidence that their information is protected from malicious intent and theft. They also protect the enterprise's brand and the company's relationship with its customers.

And, as organizations are retaining more and more data – from email to instant messages to voicemails – we need to be more aggressive in ensuring that information is protected. In Europe, the EU has harmonized its data retention laws and included a provision that the data be retained in a secure manner.

I don't think businesses should wait for regulators to tell them what to do. Instead, they should actively look for ways to protect personal or confidential data. From customer credit cards to medical records and company spreadsheets, databases hold the most critical information in the enterprise.

That's why the Symantec Research Labs team has been working on a new database protection technology called Symantec Database Audit and Security. This technology can monitor every database transaction – in real time – building an audit trail, scanning for anomalies in the usage patterns for each database user, and flagging sensitive data requests that don't comply with company policy.

Managing security risk is just part of keeping information safe. We also must make sure that it's backed-up and easily recovered. In fact, it's critical for enterprises to put backup and recovery solutions in place so that customers don't lose access to their information for even a moment – or worse, for good.

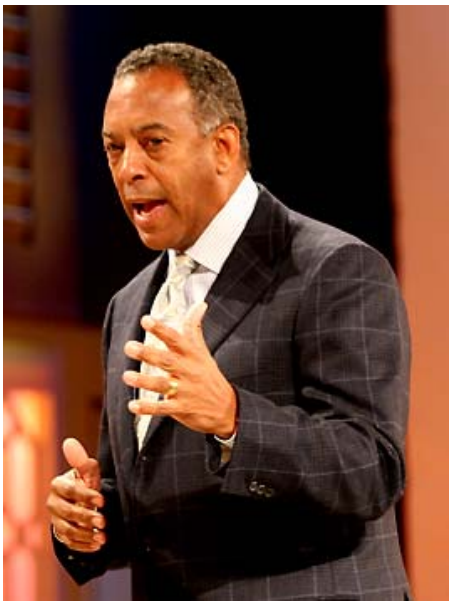
After all, no one wants to have to explain to a mother that you lost all her family pictures or to alert a small business that their financial records no longer exist.

The next logical step is joining together to create a trusted online community. One that provides end-users with a convenient, seamless, and safe online experience.

Think about it.

In the physical world, it's easy to walk into a store and get a sense of what kind of place it is. Does the sales person know what they are talking about? Are they trying to sell you an old floor model? You get a feeling about whether it's smart to give them your business – much less your credit card.

We have a sixth sense in the physical world. But, right now, we don't have it in the online world.



"It's up to the business community to assess what's safe, protect online interactions, and make sure data is secure and available."

So, it's up to the business community to assess what's safe, protect online interactions, and make sure data is secure and available. We need to help consumers develop their online sixth sense.

That is the only way the digital lifestyle will continue to be embraced.

As I said before, at the foundation of this trusted community should be a process in which customers and businesses can authenticate their identities to each other. That way, businesses can be confident that "you are you," and -- in turn -- you can be confident that "they are they."

Using a computer or smartphone, a consumer can access his accounts, be authenticated as real, and trust that the information is accurate.

A trusted community also requires a way to search the online world safely. How many times have you conducted a search, and not recognized the site that comes up? Or, visited a site you think you know only to wonder if it's really a fake Web site designed to steal your personal information.

You have no way of knowing whether a site poses a threat to you and your information.

So, you click, and you hope.

Now, imagine if the site's safety and security were checked out ahead of time, by a company like Symantec. And the site's credibility was confirmed right there in the search results.

So, when you searched the Web, the content and commerce sites came with a credibility rating – one that is updated by users who are a part of the community. This process would help give consumers that online sixth sense.

Building this trusted community will go a long way to restoring confidence by ensuring that the interactions and information are protected. More important, it will protect the relationships – the partnerships between customers and businesses – that are so critical to our digital lifestyle.

All of us in the IT industry – and in the business community – need to take the lead in pushing for policy changes that will protect privacy and critical information. And, we also need to ensure that the laws provide some protection for enterprises that have taken reasonable steps to protect their customers.

To start, the business community must join together to push for comprehensive privacy legislation.

Some governments have already stepped up to the plate. However, up until now, the U.S. government has been reactive – dealing with important parts of the issue on a piecemeal basis. Currently, U.S. privacy regulations focus on sensitive areas such as financial and health care information and protecting children online.

It's an approach that, ultimately, will result in a number of different, confusing regulations. In light of the growth in identity theft and the rise of invasive threats like spyware, we need a comprehensive response that ensures that information is protected at every step along the way.

In this country, we need one, national data-breach law. Instead of a patchwork quilt of state laws, we need one federal law that protects all consumers from data breaches and encourages innovation in data security technologies.

I'll leave the details to the lawyers. But, to me, an effective data-breach law would require notification to the affected consumer and would include tough enforcement policies. It might also require enterprises to put in place some type of reasonable security measures.

Because our businesses are part of a global community we need to ensure that conflicting regulations don't hold back the global economy. We need uniform laws and greater international cooperation to fight cyber crimes and prosecute cyber criminals.

Whether it's helping to craft new legislation, integrating security into service offerings, or creating a trusted online community, the challenge before every business leader is enormous. The future of the digital lifestyle and the digital economy is in our hands.

Trust is the foundation of this new world.

With millions of people relying on the digital world to work and play, no company operating in virtually any industry can ignore the safety of their digital interactions.

Because every time there's a data breach, identity theft, or any type of online crime, it undermines trust in your brand, in your business, and – ultimately – confidence in the entire digital world.

Lack of confidence threatens the very future of the digital environment that businesses are counting on for future growth and profitability – and that consumers are counting on so that they can enjoy the ease of the digital lifestyle.

So, it's incumbent– not just on security companies or security professionals – but on all of us to make information assurance a top priority.

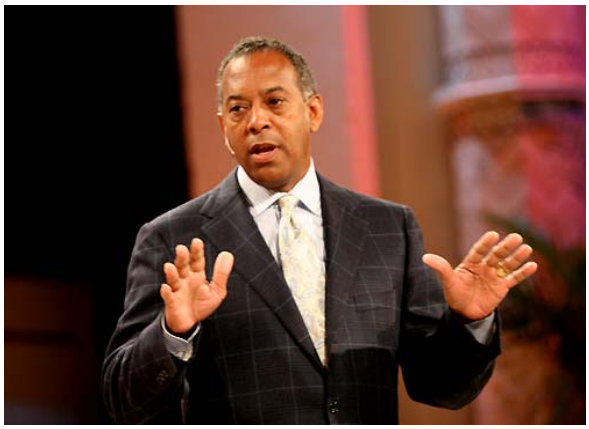
With online banking accounting for half of the transactions at some banks, it's the banking industry's concern too.

With credit card companies processing billions of consumer transactions a year, protecting personal information also must be on their agenda.

And, with the healthcare industry moving more and more patient information online, they too need to focus on protection.

We must join together and take responsibility for the digital world that we have created, because it will thrive only if we do more to give our customers confidence.

We must reach beyond the walls of our individual companies and work with our customers to deliver comprehensive, end-to-end solutions that are right for them.



"We must continue to develop state-of-the art technologies that will protect customers from tomorrow's challenges and enable them to take advantage of tomorrow's opportunities."

We must continue to educate consumers and enterprises about the changing threat landscape. We must continue to invest in research and development projects. And, we must continue to develop state-of-the art technologies that will protect customers from tomorrow's challenges and enable them to take advantage of tomorrow's opportunities.

If we do that, if we raise our sights to the opportunities that lie ahead, I have no doubt that we can build trust, create confidence, and enable millions of people to safely enjoy the convenience, the power, and the possibilities of the digital world.

Thank you.