

**INFORMATION-CENTRIC SECURITY: THE NEXT WAVE**  
**Remarks by John W. Thompson**  
**Chairman and CEO, Symantec Corporation**  
**RSA CONFERENCE 2008**  
**Remarks As Prepared with Q&A – April 8, 2008**

---

It's a pleasure to be here again at the RSA Conference. Each year, I look forward to speaking to this group because it gives us an opportunity to take stock in our industry – where we've been and where we're going.

Understanding the future is the holy grail for any business. Those that can make sense of today's trends are valuable to any enterprise trying to plan for tomorrow – or five years from now.

That's why I was so struck by a *Wall Street Journal* article I read back in January. It did something we almost never see: it dusted off old predictions to see how they panned out. In this case, the *Journal* revisited predictions that Silicon Valley leaders made in 1998 about what the world would look like in 10 years.

By and large, this group got a lot right – about computing speed and Internet access, to name just two. But, they were off in how people would use these new technologies.

They predicted that cell phone penetration in the United States, for example, would jump from 20 percent to 51 percent. Today, it's 84 percent. They didn't see the rise of high-tech outsourcing to places like India. And they believed that come 2008, personal checks would still be the dominant form of non-cash payment – which it isn't.

Now, before we pass judgment about these experts' forecasting skills, let's consider what the attendees at the RSA Conference back then would have said the biggest security concerns would be in 2008.

Most likely, they would have focused on the threats we saw then becoming more severe – increasingly complex viruses targeting individual machines, more attacks against emerging platforms like Java, and an explosion of new macro viruses infecting documents and spreadsheets.

What we probably would not have anticipated was how much the landscape would change in 10 years. While many of those risks are still around today, the frontlines have shifted. The battleground for security no longer revolves around the infrastructure. It now revolves around information – which is unquestionably our most important asset.

Today, IT organizations are dealing with petabytes of data – and, the amount is growing exponentially every year. It's a wide, open world, and confidential information is everywhere.

Think about this stat for a second – some say as many as one out of every two USB drives contains confidential information. Or consider this: as much as 75 percent of corporate intellectual property is accessible either directly or indirectly via e-mail and other messaging applications.

Information is as distributed and mobile as today's workforce. It lives in hard-to-protect unstructured formats – e-mail, spreadsheets, and instant messages. And as software-as-a-service continues to grow, your most sensitive data – more often than not – will be found in the “cloud.”

In our new world, the risks to information are real – and growing.

The Symantec Internet Security Threat Report, which was just released this morning, provides a real look into this problem.

I'd like to have Steve Trilling, our vice president of Security Technology and Response...and the person who manages all our research on new and emerging threats...join me on stage to talk about the findings.

**John #1:** Can you tell us where the data in the Internet Security Report comes from?

**Steve #1:** John, We have some of the most comprehensive sources of Internet threat data in the world. Just to give you some examples, we get malicious code reports from more than 120 million computers running our software; we have 40,000 network sensors in over 180 countries; and we're tracking vulnerabilities in more than 50,000 different products. All of these data sources really give us a strong global picture of attack activity on the Internet.

**John #2:** I'm talking today about protecting information. What are the main causes of information leakage that we're seeing?

**Steve #2:** So the number one way people are getting hit is through theft or loss of laptops and storage devices. We're talking about someone leaving one of those USB drives that you mentioned, on an airplane, or a hard drive with confidential data that's unencrypted getting stolen from a company – and taken all together, these kind of problems make up 57% of the data loss we're seeing.

Another reason companies lose information is because they don't set up appropriate security policies – even simple things like telling employees not to send work documents to their personal email.

As you know, we've been talking about hacking and insider attacks for awhile – these also continue to be problems...So overall, we think a lot of these losses are very preventable if you have the right tools.

**John #3:** Is malicious code a problem in this area?

**Steve #3:** Yes, and this isn't your mom's malicious code anymore. To give you some perspective, during the last 6 months of 2007 nearly 70% of the most common malicious code threats we received into our lab, steal confidential information. That means they log keystrokes, they grab passwords, they take account information, and send all of this off your computer to a remote attacker. And something else interesting, at least I think it's interesting, is that for the first time, we think we've reached an inflection point where there is more malicious software being created every day than legitimate software.

We conducted a study and found that 65% of all unique software programs released to users were characterized as malicious – and the fact that most of these threats are going after your personal data is pretty worrying.

**John #4:** So what do the attackers do with all this data they are stealing?

**Steve #4:** There is actually an entire underground marketplace that has developed to sell information stolen on the Internet. It has all the workings of a full economy - they have mechanisms to advertise the data to potential buyers, they have people who handle money transfers, there are even people who can accept items ordered from a stolen account. It's really pretty sophisticated.

**John #5:** And what types of data can someone buy here?

**Steve #5:** There are all kinds of stolen items available for sale. As an example, online auction accounts go for up to 8 bucks. Email passwords are worth a little more, they sell for up to 30 bucks. A bank account that has a lot of money in it goes for 1000 dollars. On the flip side, someone can buy your credit card number for as little as 40 cents...of course; the upside is there's always the small chance they'll take over your payments.

**John #6:** We've heard a lot about traditional financial data theft, what other types of theft are we seeing?

**Steve #6:** Well I'm not a gamer, which I'm sure comes as some surprise, but it turns out that a stolen account to the online game World of Warcraft is another popular item in the underground economy. Some of these accounts go for 100 times more than a credit card. Who would have guessed that the High Warlord's Thunderfist is more valuable than your platinum card?

**John #7:** The High Warlord's Thunderfist?

**Steve #7:** I believe it's a weapon for killing goblins...now you can understand why it's worth so much. But the serious point here is that even in these virtual worlds, there is real money for attackers.

**John #8:** How about identity theft, is this still an issue?

**Steve #8:** Absolutely – stolen identities were the third most advertised item we found in our study of the underground economy, during the last 6 months of 2007.

Nearly 50 million people around the world had their identities exposed during this period. That's 3 identities lost every second for 6 months...really an unbelievable number.

**John #9:** So with people buying and selling this stolen information online, why can't law enforcement just shut these channels down?

**Steve #9:** This is not an easy problem for law enforcement. Most of these transactions take place on public chat servers that can be hosted virtually anywhere in the world, and the criminals themselves can be anywhere.

So, when authorities do discover this type of activity and shut the channel down, the criminals just go to another chat room on another server somewhere else and keep doing business.

**John #10:** So we've talked about the data that attackers are stealing and selling. Do we know anything about which particular sectors get hit the most?

**Steve #10:** We do look at this. Education was the most affected sector during our study period, with 24% of the data breaches, followed closely by Government, with 20%.

Healthcare and Financial Institutions were next on the list. The interesting thing is that, while the government sector accounted for 20% of the total data breaches, those breaches led to 60% of the identities exposed during the period.

Hey, who says government isn't efficient?

**John #11:** This is why I outsource my humor.

**Steve #11:** Thanks John, I always appreciate your candor.

I'd like to share another stat with you.

According to the Privacy Rights Clearinghouse, the number of exposed records tripled last year. From the high-profile breaches that are splashed on the front pages to the smaller ones that we never hear about, millions of consumers are affected each year.

If ever there was a cry for a change in public policy, the time would be now. It's impractical to have 40 states – each with its own data security laws.

I am glad that policymakers are realizing how important protecting consumers' personal information is, but what we really need is a federal law that will set one, high standard to protect consumers regardless of where they live...and to make doing business easier across the entire United States.

Whether it's plugging the flow of data breaches, protecting people's privacy, or integrating cybersecurity into any plan to protect our critical infrastructure, we need to recognize that these are problems not limited to one state, one country, or even one continent.

These are global problems that require, at the very least, the attention of the entire IT industry. That's why today we announced the merger of the Cyber Security Industry Alliance into the Information Technology Association of America.

This move will give CSIA a bigger platform and a stronger voice on these critical public policy issues and the ability to work with governments and key stakeholders around the world.

I applaud this merger because time is of the essence. We need to move quickly – on the policy and technology fronts – to protect information because right now, too many organizations are leaking critical data like a rusty bucket. And it's costing real money.

According to the Ponemon Institute, the average cost per compromised record is just under \$200. They also put the average cost per breach at \$6.3 million in legal and PR fees – and lost business.

In the past, our reaction would have been simple: build higher and stronger walls.

But today, you can't do that and have a successful business. Decision-making depends on access to information. So, we must rethink our approach to security.

Now, I know that making predictions can be really risky. The last thing I'd want is anyone waving them in my face 10 years from now. But, I'm willing to take that risk.

From where I sit, a few things are clear:

- If the growth of malicious software continues to outpace the growth of legitimate software, techniques like whitelisting – where we identify and allow only the good stuff to come in – will become critical.
- Identity management will only grow in importance. And we'll need to expand it beyond the boundaries of an enterprise environment to include every consumer in the world.
- And digital rights management will start to become a reality. And I'm not talking about music and video, but important digital content that drives your business day in and day out.

We need to think about how to use today's tools to set us on the right path. I believe this starts with a fundamental shift toward an information-centric view of security.

I'm sure you're asking, what do I mean by that?

Information-centric security is about taking a risk-based approach to protecting confidential information. With the amount of stored data growing 50 percent a year, trying to protect it all is both inefficient and costly. Instead, it's about securing the most critical information – from source code to customer information to employee data.

It's about balancing risk and opportunity. It's about protecting data at rest...data in motion...and data in use.

We are seeing the contours of information-centric security take shape now. It starts with you being able to answer a few simple – but important - questions.

First, what sensitive information do I have?

Next, where is that sensitive information stored?

And finally, how is the information being used – both on the network and at the endpoints?

Once you gain insight into how your information is being used, you can begin to set policies that help you mitigate your risks.

And I'm not talking about a handbook that sits in the top drawer of everyone's desk and is read once – if ever.

These policies are the strategies that guide how your organization uses information – and secures it.

They set rules for things such as storage-tiering, archiving, and encryption. For example, you might decide that your employees can copy data to a USB drive – but only if the drive is encrypted. Or you might decide that confidential information about employees can't be sent via e-mail.

The policy nuances are endless. But what is constant is that these policies must be aligned across the company. Your information security policy needs to be consistent with how you want to run every aspect of your business – from managing HR records to partner information and customer data.

That's why I believe your business leaders must be involved in setting the policies – not just the CIO, but the CFO, and the COO...people up and down and across the organization's executive suite. After all, if security is meant to be a business enabler, then those that run your business must be involved in setting the rules of the road.

Beyond that, executive involvement is critical to fostering a culture of security.

I was struck by a visit to a major New York bank recently. In the lobby, was a large poster that lays out the key points of their information security policy.

What a great way to make expectations clear and remind employees – each and every day – of the important role they play.

And that's what we need: a society in which the value of information – both business and personal – is understood, and in which all of us work to protect it.

If policies are the strategies we use to secure and manage information, then technologies are the tactics used to implement and enforce them.

Traditional security solutions – antivirus software, content filtering, and anti-spam programs – remain important.

But, that's no longer enough – we need to be able to protect information wherever it is.

Doing that requires security and data management solutions to work hand-in-hand – and as part of a broader information risk management initiative.

Years ago, we imagined a world where intelligence about an emerging threat could trigger an automatic backup – just like the Doppler radar tells you that a storm is coming and you need to close your hurricane shutters and batten down the hatches.

Not long ago, this became a reality as our ThreatCon global security alerting system was integrated with our Backup Exec family of products, enabling backups to be triggered automatically by heightened security threat levels.

More recently, we talked about being able to discover exposed confidential information on the endpoint and automatically move it to an encrypted storage location. In its place, it would leave a stub – kind of like a ticket at a coat check – to let the user know that the data has been moved and where to find it.

With the Data Loss Prevention solution we recently acquired from Vontu, we now offer this to customers.

OK, I know I'm not supposed to plug our products, but I can't help it...this is really great stuff.

When I look at what we offer and compare it to where we – and the entire industry – were a decade ago, it's clear that we've come a long way in the past 10 years.

We've started to recognize the business value of our information. We've recognized that security and data management are inextricably linked and together are the core of an information-centric approach to security.

But, it's not good enough. We need to take it to the next level.

I believe that in five to 10 years we'll get to a system that marries security and information in a more complete and holistic way. As we enable enterprises to gain knowledge of their content, knowledge of their users and knowledge of all of the devices on their network, we'll see an enterprise rights management system emerge.

But to reach that goal, we need to do more around content awareness. Today, we have the basic building blocks in place to accurately identify confidential information on file systems, databases, and desktops.

We need to extend these capabilities more deeply into the mobile environment. Today, we can see what information is being sent from a BlackBerry over the corporate network. But there are still gaps – someone could use their BlackBerry to send confidential data over their personal Yahoo account or download it onto a memory card. And you can't see it or stop it.

Being content aware also enables us to do more around the concept of intelligent archiving.

We can make smarter decisions about archiving information – whether it's storing information that needs to be retrieved regularly on disk...encrypting highly-sensitive information, such as your financials, automatically....or deleting all the spam and stupid jokes that don't need to be archived at all.

In the end, this enables you to archive only the key data and save on the rapidly growing storage costs.

Moving forward, advances in content awareness will be critical to enhancing information-centric security solutions.

As I mentioned earlier, making predictions is a tough business. But making sense of the future is what we all strive for.

And, as I look at the future of security, the path ahead is pretty clear.

What's needed now – and in the years to come – is a broad set of policies and solutions that can enable a true information-centric approach to security.

The bottom line is: you can't secure what you don't manage.

Of course, there are still those that fail to see this future. They are still focused on protecting the network or providing point solutions to keep threats at bay. They are fighting yesterday's battle.

What organizations need instead is to look ahead – to embark on a longer-term journey that orients the entire organization around an information-centric security program.

I know this won't be easy – change like this never is. But, it's time to start making decisions about how to realign our organizations around this new goal.

Many of us have made great strides in aligning IT more strongly with our businesses. As a result, IT has gained a wealth of cross-functional knowledge about the organization. Now it's time to leverage your expertise to become trusted advisors to the business...to partner with the business leaders to formulate the best policies to manage the business and its information.

That will require you to think more holistically about the whole process – from developing policies to training staff and finding the right set of technology solutions.

Ultimately, the work of protecting business information is everybody's job – not just IT's.

It's a challenge all of us must tackle in order for our businesses to thrive...to become more agile and high-performing...and to realize the full promise of the connected world.

Working together, as an industry, I know we can meet this challenge.

Thank you.