Stanford eCorner

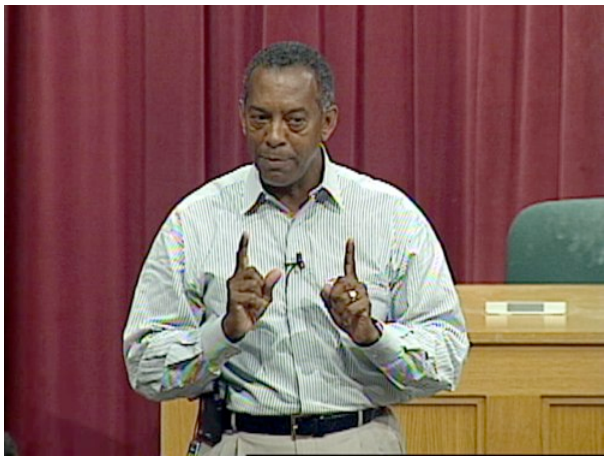
Security Business Post-9/11

John Thompson, *Symantec Corporation*

May 23, 2003

Video URL: http://ecorner.stanford.edu/videos/351/Security-Business-Post-911

Thompson talks about how the most significant event for the security space was not 9/11 but it was 9/18. That is the day a dangerous virus, nimda, hit.



Transcript

Final point. Many people have said, "Gee, post 9/11, the security business must be incredible!" And the reality is the most significant event that occurred in the security space was not September 11th, 2001. But it occurred on September 18th, seven days after the attack on the World Trade Center and the Pentagon. And it was a voracious virus or worm known as "Nimda". And what Nimda did was it raised the ante for how security will be deployed by individuals and enterprises be they public or private enterprises around the world. And what it forced people to concentrate on or think about was first business continuity. In the event that something does go wrong, how will I ensure that my business will continue to operate? And then second, to the extent that I have deployed some of these technologies that have been talked about, how do I know that I am as secure as I am. Because no one or single technology at any single tear of the network is sufficient to be able to deal with the kinds of aggressive threats that we see being posed in the network world. We used to get on average 1,000 to 1,500 submissions of suspicious files into our laboratories every month. Today we get over 100,000 submissions a month.

What it says is that the level of activity has not only increased, but more importantly and candidly a bit more scary is the complexity of what we are finding is starting to increase exponentially. Case in point, the most recent aggressive worm that we've seen was called "Slammer." And Slammer affected almost 300,000 systems in 15 minutes. And so many of the classic forms of security technologies that we have been involved in at Symantec and many other companies around the world are finding that that approach to security is not adequate in today's network economy. And so we've approached it from the point of view that it's an end to end process that has some products that are a part of it. But it is a business process that has to be deployed if in fact you're going to ensure that you can create a very, very secure systems infrastructure. It's an exciting time, this is probably the hottest market in the IT segment right now. It's projected to grow somewhere in the range of 17% to 19%. It will be just the part that we play in will be a $10 billion business if you add the services components on top of that, it will be a $27 billion business this year. And so I think our little company has a chance to make our little $1.6 billion if we execute well day in and day out. But it's been a wonderful time being at Symantec and watching not just the changes in the valley but more importantly, the changes in customers' attitudes about what we can do to help them solve the problem and be more confident in their interactions in a wired world.

Because it's clear that the clock will never go back to an unwired environment and so what we have to do is create the sense of confidence that I can operate in a wired world without fear of my credit card being stolen, without fear of my identity being stolen, without fear of people hacking into my systems and taking money or moving it from account to account. While those things are all possible, I think our job here is to make sure that they are not as probable tomorrow as they might be

today. So let me stop there and see if I can answer questions.