Enrique Salem RSA 2011 Keynote

Good morning.

I'd like you to join me as I step back into time.

Way back to July 13th, 2010.

It started off as an ordinary Tuesday.

For avid cyclists like me, it was another day of wondering how Lance Armstrong would do after another vicious crash in the Tour de France.

Math geeks and puzzle lovers were celebrating the birthday of Erno Rubik, inventor of the Rubik's cube.

In the Gulf of Mexico, it was day 85 of that tragic oil spill.

But for many of us here today, the really big news of July 13, 2010, didn't make headlines. Or the national news.

Yet, for the global security community, July 13th turned out to be a pretty significant day. Even if we didn't quite know it then.

For it was on that day we first got word – via an infected computer in the Ukraine – of a new worm that the rest of the world would soon know as: Stuxnet.

STUXNET

From our very first glimpse, everything about Stuxnet appeared suspicious.

How and where it exploited the host.

The sheer size of the thing. It was over a half a megabyte of pure code.

The fact that it contained SCADA strings.

The unusual geographic spread of infected hosts.

We quickly started to reverse engineer this very unusual worm.

At the same time, we were also able to identify its command and control servers. There was one in Denmark and one in Malaysia. We managed to switch the command and control from those servers to a Symantec-controlled host in Ireland.

This gave us a unique visibility into Stuxnet. We could see the infected machines. We eventually discovered almost 100,000 infected hosts.

As we learned who was infected, we reached out to those organizations and assisted them, regardless of whether or not they were our customers.

It was a comprehensive "special teams" approach that went well beyond what any other security

company did or, frankly, was even capable of doing.

Let's face it. We are all being bombarded by 2 million threats a day.

The real skill is differentiating the standard threats from the significant ones and acting accordingly.

And Stuxnet proved to be very, *very* significant.

Stuxnet had four zero day vulnerabilities. One zero day vulnerability is big. Four is huge. And unprecedented.

At Symantec, we helped unmask three of those vulnerabilities.

Stuxnet had two PLC-specific vulnerabilities:

One was the first malicious STL (Statement List) code designed for the purpose of taking over industrial control systems.

And the other was the first-ever PLC rootkit to hide that STL code.

Stuxnet also used two stolen certificates from innocent third parties to sign its files. That was another first.

And finally, it had seven, *seven* forms of replication. The average malware program has one, rarely two. Again, unprecedented.

Any one of these characteristics is noteworthy on its own, but combined, they create a very special weapon.

It was sophisticated. Elaborate. And as we were about to learn: meant to destroy.

In fact, Stuxnet will always be remembered as the malware that changed the game from espionage to sabotage.

All technical evidence to date suggests Stuxnet is the first virtual weapon designed to destroy a physical environment.

Stuxnet targeted a specific group of programmable industrial controllers. Controllers like this.

Many now believe that Stuxnet took command of controllers just like these and triggered a series of events that caused a very specific set of uranium-enrichment centrifuges in a very specific Iranian nuclear facility to spin at such high rates of speed that they literally destroyed themselves.

How could an attack like this happen inside a secure and well-monitored nuclear facility?

It seems Stuxnet also employed the first rule of the Art of War: deception.

The theory is that Stuxnet recorded console readings of normal operations at the nuclear facility, and then played them back while the centrifuges were tearing themselves apart.

It's like a scene from a bank robbery film where the guards at the security console are fooled by a fake tape.

Of course, the noise at some point would have told them not to believe the readings they were seeing. But if they did go for the "kill switch," we know that Stuxnet appears to have been able to disable that as well.

Remember: Sophisticated. Elaborate. Meant to destroy.

News reports say that Stuxnet wiped out a fifth of Iran's nuclear centrifuges and set back their development schedule by several years.

As security professionals, we have been expecting something like Stuxnet for some time and now we will all have to deal with the profound implications it has for us.

SCADA attacks are not new. You might recall the case in Siberia where a compromised industrial control system resulted in the explosion of a natural gas line.

But imagine if Stuxnet's target had not been uranium-enrichment centrifuges, but something more explosive. Say a target in France, Japan, or California.

Imagine a new wave of threats in which the hands of criminals and zealots reach out from the safety of cyberspace and wreak real, physical damage, destroying not only information but actual physical property.

This represents not just a threat to our economy and our prosperity. It represents a very real threat to people's lives, and our way of life.

But whatever its real target or its degree of success, we now know what Stuxnet is capable of.

And history has taught us that inevitably others will use Stuxnet as a starting point for their own, potentially even more lethal, threats.

And so, we continue to watch, and track what Stuxnet is doing.

This is the brave new world we live in.

At Symantec, like all of the professionals in this room, we take this very seriously.

We view our role as the world's largest security company as an enormous responsibility.

Individuals, companies, and governments around the world rely on us to keep their information, infrastructures, and interactions safe and secure.

But more dangerous and ever more technically sophisticated threats are only one of the megatrends that are redefining the security landscape.

TODAY'S MEGATRENDS

For years I have spoken to you about the consumerization of IT, of users bringing more of their own devices and their own technology habits into the workplace. This is being driven by the massive proliferation of mobile devices programmed for data access, whether they are authorized or not.

And this feeds into social media. It's being accessed in the workplace. It's being used for work in the workplace. It's only going to increase.

There's the continuing data explosion that is causing information storage and backups to increase by as much as 52 percent year over year.

Then there is virtualization. A trend that is well past the early majority stage. Analysts believe that by 2015, 60 to 70 percent of servers will be virtualized.

And of course, there's the cloud. Public and private. And we'll talk more about the implications of all that.

Like the technical specs of Stuxnet, each one of these megatrends is noteworthy on its own.

But taken together, they might suggest that like a certain set of uranium enrichment centrifuges, things are beginning to spin out of control.

LOSS OF CONTROL

It was not so long ago when IT professionals were securely in control of their computing environments.

You controlled the desktop. You controlled the databases, applications, and servers. You controlled the users (to the degree such a thing is actually possible).

Computer processing was done in the office, within your four walls, and you were responsible for that environment. So it was your rules.

I don't have to tell you that those days are over.

Today, as I said earlier, there are all kinds of devices coming into the office.

USB drives, notebooks, smart phones, tablets. Some of these are yours. But increasingly, many of them are not. They're being brought in by people who work for you and with you.

And they're being used for all kinds of things. Staying up on corporate email is one.

Logging on to personal Facebook and Twitter accounts is another.

It's interesting to note that social media has overtaken email by both time spent and by volume of data.

Facebook already has over 620 million users and is growing 51 percent year over year.

In fact, Facebook has surpassed Google as the number one destination on the Web in America. And social has replaced search as the primary reason for going online.

And that, of course, has created whole new gateways for threats to enter into your environment.

But it doesn't stop there.

This year, there will be more smart phones sold than desktop computers.

Actually, these aren't really phones so much as they are handheld computers wirelessly connected to the cloud.

The average cell phone usage pattern is 70 percent voice. The average iPhone usage pattern is 45 percent voice. The rest is data. And you know where it's coming from.

And that's just the crest of the tsunami that is about to descend on us.

Mobile data traffic is expected to increase by almost 4,000 percent in just the next three years.

Four. Thousand. Percent.

Soon, for millions and millions of people, a smart phone will be their primary connection to the Internet, to the cloud, and to your virtualized environments.

Of course, all of these entry points to your cloud infrastructures are also endpoints.

And as endpoints proliferate on this seemingly insane trajectory, so do the threats they attract.

Matters are made worse by today's micro-distribution model of endpoint threats. 75 percent of all malware infects fewer than 50 machines. Signature-based scanning long ago failed to keep up.

That's why reputation-based security will be critical moving forward. And not simply IP-based reputation, but a real-time, contextual tracking system that monitors dozens of file attributes such as file age, file download source, and file prevalence.

Today we are announcing the beta of Symantec Endpoint Protection 12. It is the only reputation-based security that context-aware.

We will provide telemetry from more than 175 million endpoints on over 2.5 billion active files.

These attributes are combined using a reputation calculation algorithm to determine a safety rating. As a file is distributed across the Internet and these attributes change, we will continue to monitor the file and update its ranking.

This lets you know if know if file is good *or* bad

Nobody else does this.

Of course, with the proliferation of endpoints, there is also a corresponding proliferation in the number of devices and locations where data is processed.

Let's face it: The walls have fallen off the data center.

Processing is happening everywhere.

Applications that once existed only in the physical confines of the data center are now being accessed in planes, trains, automobiles, cafes, restaurants, bars, and beaches.

Key information and applications will no longer sit inside your legacy data center under your control.

Now you will have to protect, manage, and police people and information, regardless of device and regardless of location.

Those of us responsible for this will have to adapt – and adapt quickly – to this new role.

But how?

How do we adapt with a world where devices and datacenters access information that is stored, used or passed through the cloud?

REGAINING CONTROL

At Symantec, we're no stranger to the cloud. We have been securing the cloud since its beginnings.

Today, we back up more than 60 petabytes of data into our cloud.

We protect more than 7 billion emails every month in the cloud.

We protect more than 5 million identities in the cloud every day.

Moreover, you'll find us infused throughout some of the largest clouds in the world run by organizations like Amazon, and eBay.

And we provide data loss protection gateways to many other clouds.

So how can we help you create a safer environment for your information, your interactions, and your people?

We can help you in two ways.

First, Symantec will provide protection *from within* the cloud. We will deliver a whole complement of security services that you already know and rely upon: security, backup, recovery, data loss prevention, encryption, etc., delivered as cloud-based services.

We're calling this Symantec.cloud. And many of these offerings are available today.

Second, Symantec will also provide you with security *for* the cloud.

And just as we can't protect today's proliferating devices with yesterday's endpoint protection, we can't protect the cloud with yesterday's solutions.

Our times call for a bold new approach, and here's why:

You can have chip-level security. But there will be a hack for that.

You can put security in the device. But there will be a hack for that.

You can have security in the OS. But there will be a hack for that.

You can build security into the network. But there will be hack for that.

You can even build security into your own uranium-enrichment facility. But there's already a hack for that.

So in this environment of rapidly changing computing paradigms and just as rapidly evolving security threats, how do you maintain control? What does that even look like?

Well, we have control when we set the rules. In IT, rules are policy. It's what we all call *governance.*

Once we have defined rules/policies/security controls, we need to be able enforce them. Is that enough? Actually, it is not.

Control is also about visibility. We need to be able to verify that all the right things are happening, that our policies were truly deployed and properly enforced. We call this *auditing* and it's critical for today's compliance regulations.

Governance. Protection. And visibility. It is only with these three ***combined*** layers can we achieve control, confidence, and trust.

So how are these things achievable in the cloud?

Maybe the cloud metaphor can actually be useful here as something more than just a handle for analysts, a marketing gimmick, or a graphic cartoon.

What's actually above the clouds?

A layer of protection called the *ozone.* It shields the earth from harmful elements and the effects of the sun. And interestingly, it's made up of three molecules of oxygen.

With that as context, I'd like to introduce a concept we are developing at Symantec. We call it "O3."

Like the real ozone, its goal is to protect us.

And like the Earth's ozone, it is composed of three distinct pieces that work together to solve the challenges facing us in this new borderless enterprise.

Let me describe how this architecture works. There are three layers.

The first layer is a policy engine where you create the policies and rules that govern your people, devices, and information in the cloud.

This is important to note: this approach will let you put your legacy corporate identities to work for you in the cloud. These are the identities you already own and control. There is no need to give control to a third party or to start from scratch. Each legitimate employee or identity has their own password that allows them to access whatever corporate assets they are legitimately entitled to as well as their own social media networks and e-commerce sites.

In addition to identities, you can create rules for devices, even permissions for networks as to what sort of information they are allowed to transport and what information they are not.

The second layer is the protection or enforcement layer. This is where your employees and devices are authenticated before they gain access to the cloud. This is where the rules in your policy engine come into play.

Is this identity correct? What is the device? Is it approved? Does it have antivirus? It's an OS device…does it have the latest security patch? Does this identity have access to that kind of information? Is this network safe for the transport of that information?

Every identity, every device, and every piece of information is authenticated and policed so that you know your infrastructure, information, and interactions in the cloud are safe and secure.

The third layer is the monitoring and compliance layer. This gives you visibility into how your policies are being enforced, lets you document and report for the purposes of compliance.

And it provides you with an almost business intelligence–like platform for managing your security, regardless of platform, OS, or device.

Now you not only have a more secure cloud environment, you have a way to gain insight into an even more secure future.

This approach lets you regain control of your environment by giving you a unified architecture consisting of a policy engine that lets you determine and set the rules for every individual, device, and interaction; a security layer that enforces your rules and authenticates your identities, devices, and information; and a monitoring layer that simplifies reporting and facilitates compliance while giving you visibility into how your governance is being enforced and managed.

This is our vision for the future of security.

One that makes clouds secure, too.

We believe in this approach, and we are developing it.

LET'S REVIEW

So before I leave you, let's review.

As Stuxnet amply demonstrated to us all, the threats we are all tasked with combating are getting more sophisticated, more dangerous, and more prevalent all the time.

Especially those targeted to our critical infrastructure. In fact, Symantec is working with some of the largest manufactures of these types of systems, including Siemens.

And let's not forget WikiLeaks and the kind of damage that can be caused by something as innocuous as a simple human mistake or as dangerous as a disgruntled employee, vendor, or partner.

This is our brave new world. One where devices will soon be more prevalent than PC's. Where the walls have come off the data center, and many parts are moving to clouds – public or private.

The only option in the face of these changes is to embrace them. And leverage the new solutions. Because we can't apply the old approaches to this new world. That is the best opportunity to regain control.

As security providers, we have the responsibility to deliver these solutions to you. I've discussed our approach. But any approach must answer how we help you manage security, policies, governance, and auditing.

And you have every right to demand those solutions from us.

But we never forget, we're all in this together.

Because, Stuxnet – and whatever's next – is still out there and waiting for all of us.

Thank you for your time.

