Symantec Financial Analyst Day 2015
April 17, 2015

Helyn Corcos: I just have a few comments for you and then we'll get started. As you know, we will have plenty of forward-looking comments in today's presentations. There'll be risks and uncertainties related to those. You can find our definitions behind those in our filings with the SEC, and in addition, as you know, we also provide some of our metrics in non-GAAP form as well as GAAP, and the reconciliation of those items can be found on our website as well as in the Appendix of the financial presentation.

Now I'll just move on to a few housekeeping items before we get started. A few things today that I want to highlight is, first and foremost, we are reiterating our guidance for Q4 and the fiscal year. With regards to the comments we're going to make about Fiscal 15 during the presentation today, wanted to let you know that that's going to be based on three-quarters of actuals and the midpoint of the guidance that we had given for the quarter.

Lastly, I'm going to move on to the actual legal separation of the information management business is expected to occur on January 2nd. The first day of trading will actually occur on January 4th.

Lastly, what I'm going to do is there's a few terms some of which may make sense to you and others we just want to make sure you understand, is when we refer to Veritas that actually refers to the information management segment and the same thing with the consumer business, we're Norton. Those are used simultaneously. With regard to Symantec security, that really refers to the consumer security business as well as our enterprise security business, and then when we refer to Symantec for '16 and '17, it's really sort of a pro forma Symantec. As you know, post-separation we will actually be having—the information management business will be actually presented as a discontinued operation. You'll see that in our filing information later in the year.

So those are just some of the housekeeping items I wanted to set up front, and now what I would love to do is just briefly go through what you're going to be seeing today. We're going to start out with our strategic overview from our CEO. Then we'll move into an overview of the Veritas or information management business from our team there. We'll have a short break and then we will do an overview of the consumer business and then we will have the enterprise security team come up and give you guys a presentation on their strategy and product roadmap. We'll also then have a short break and then move into the financial objectives for the fiscal '16 and '17 periods. Then we'll end the day with Mike and Thomas doing a final Q&A.

So without further ado, it's my pleasure to introduce to you our President and CEO Mike Brown.

Michael Brown: Thank you, Helyn. Good morning and let me add my welcome. We really appreciate the time that you're spending with us today to learn more about our business and we're excited to share what we see for Symantec FY16 and beyond, because as you know we haven't been able to really talk about the business beyond FY15.

Let me start by saying I'm personally more excited about our prospects than I was even seven months ago when the Board named me to this role permanently, and let me share with you why I feel that way. First of all, in October we announced strategies for our two businesses—Symantec, going forward, and Veritas—but now we've complemented that with very detailed plans for execution for FY16. That's what you're going to see in our presentation today. So that combination of the strategy now backed by the detail of what we need to get accomplished in FY16 makes me pretty excited about what we intend to deliver for FY16.

Second, it's a new team leading Symantec these days and I was just counting, of the eight presenters that you're going to see today, basically only one person was with the Management Team more than a year ago. So a brand new team and I'm going to talk a little bit about the new team.

The presenter, you'll see, who's been with the Company the longest—four years—is Fran Rosch. Maybe you can wave, Fran. He leads the Norton consumer business. So we'll talk a little bit more coming up about the new Management Team.

Third, the momentum that we have built, especially as we've gotten into the back half of FY15, we carry forward into FY16, and I'll give you some statistics coming up that show you what I mean about that momentum, but that's what gives us confidence that it's time for Symantec to grow again. So our task for this year is to begin that growth as opposed to just working on the profitability. In fact, we've already put a lot of the things in place and shifted our investments so that we can grow as we look at FY16 and '17. That's what you'll be hearing about a lot as we go through today's presentation. So, let's get started.

I'm basically going to take a quick look back, so we'll talk about what progress did we make in this first year of what I'd say is a two to three year turnaround for the business and the turnaround is all about reinvigorating growth. What are some of the different market dynamics and why did that lead to the separation? What are the strategies for Veritas and Symantec? Then how do we leverage the scale that we have at Symantec to drive innovation and growth? We'll talk about those growth drivers.

So let's start with where the year began. When Thomas and I did the first earnings call which was in May last year, we said there were five key operational priorities that we need to drive the business. It was way too early to talk about strategy, and I'll come back and make a couple of comments about that in a moment. But the five key priorities that we set out were, number one—off to the far left—we need to optimize the portfolio of businesses and look at the business as a series of businesses, and be very transparent with you about which businesses are intended for growth and which ones are intended for margin and cash flow. As you know, some of the most significant decisions around that were the fact that our Norton business was a business, because of its lifecycle, that at this stage makes sense to optimize for margin, which we've done, and the enterprise security business, given the market dynamics, is primed for growth. We needed to do the right things to get that growth started. So that was number one.

Number two, to get after growth we've got to reprioritize the investments to go after the higher growth market areas. So you see that highlighted.

Our third, cost structure. We felt that there was significant opportunity to improve the cost structure at Symantec, so as you'll recall, we launched eight different initiatives to focus on revenue and cost.

Our fourth was we needed to strengthen the Management Team. We had had way too much management turnover.

And the fifth was continue what we'd begun, to return significant cash to shareholders through dividends and share repurchase.

One of the things we knew we needed to get going on is what you see in the lower right which is strategy. So we knew that we needed to undertake an effort to say what is the long-term strategy? We were not happy with the efforts that were in place at that time as it relates to strategy, and so we began an effort right at that same time. It was way to early to start talking about in May but now you know the results of that. So let's look at what happened in FY15 as a result of these different priorities that we set.

So first, if we look off to the left, this is the momentum that I was talking about. We set expectations that growth would be relatively flat for the year. What we did see is because of the things that we started working on, we see a lot of momentum in the business. These indicators, we think, are kind of the leading or forward indicators for the business and imply growth for FY16. So first is implied billings. That went from negative to a positive. Thomas will give you a little more detail on that in his presentation, but for FY15 that will be positive 3%.

Most of our revenue in the current quarter, as you know, comes from the balance sheet. So the second metric there refers to deferred revenue. We had dug for ourselves as we went through FY14 quite a hole in terms of deferred revenue. Now that again is growing for the first time after six quarters. So we're very excited about the strengthening of the deferred revenue obviously combined with growth for FY16 will help us grow.

Then our Veritas business has been a bit of a standout. That not only has the positive momentum from building deferred revenue but it is actually growing and that growth rate is accelerating. So you'll hear a lot more about that as we go forward. That grew from 3% year-over-year growth in the September quarter to 5% in the December quarter, and that's not an upper limit; we expect that to continue.

So very pleased about the momentum that we're building as we drive into FY16. That momentum is not just on the revenue side but also the operating margin side. So if you start at the far right, those eight different initiatives that we talked about, they delivered over $150 million in additional profit or upgrading margin this year. That's what led to—if you look to the left—margin expansion that led us to as a total company hit the goal that we set of 30% operating margin by our third quarter, the December quarter. Of course fueling that was the effort on Norton. We said we were going to optimize that business for margin and cash flow, and Fran and his team did an outstanding job there. They got that business up from 43 to 53% during the year.

When we talk about talent, there's five executives new to the Company. I'd like to just take a minute and share with you who they are here today. Thomas as you know joined at the same time I did, and most of you know him already. If we look over to your left, John Gannon joined to lead what we're now calling the Veritas business; a long-time peer at HP, a storage industry veteran. In fact John and I also worked together at Quantum. He'll be talking more about the Veritas business as we go forward.

If we look at the second row, another new addition from outside the Company, Balaji Yelamanchili. Balaji is leading our enterprise security portfolio, so all the products and services that are enterprise security. He joined from Oracle in November and he led the big data analytics business at Oracle. As we talk about the unified security strategy, you're going to see why that's incredibly relevant for us going forward.

Over if we look to your left, Amit Mital joined the Company from Microsoft. He's our Chief Technology Officer. He's also been a key person behind some of the strategy work that we did this past year.

If we look to the back of the room, Amit Jasuja, a recent addition from Oracle. He led Identity and Access Management, which you'll be hearing about when we talk about information protection going forward. He also led the Java business and IoT at Oracle. So we're delighted to have him join the team.

Jeff Scheel, who's standing, joined us to lead up Corporate Development, Strategy and Alliances. Jeff's joined us from FireEye and Mandiant, and before that he was at HP and ArcSight, adding a lot of security industry expertise to the team.

So these are the five additional executives who are here with us today. If I add our leader for worldwide sales, Adrian Jones, who joined us from Oracle; Amy Cappellanti-Wolf, a long-time Cisco person who is leading HR. We have quite a few new executives, eight or nine different new executives at the Company.

I couldn't be more enthused about this team. The capability that they bring is what we need to be able to execute as we look forward to FY16 and '17.

So a very key accomplishment there in terms of getting an assembled executive team going forward.

If you've already looked ahead on the slide, you see we continue to deliver new product. So the cadence of product delivery we were pleased with but I would say it didn't deliver enough of the innovation that we're looking for. We started investing that in FY15 and you'll see that today in the presentations.

As far as the strategy work, what we saw when looked at a complete review of the strategy, and this was some of our best technologists and strategists in the Company. We looked at some outside perspective. We hired some folks from the outside, consultants, bankers, so we got a complete view. This really led us to the conclusion that there were two different strategies that made more sense than one because we were objective enough to take a look at the Veritas business combined with Symantec and say are we really better together, or can we execute better if we approach these businesses separately? You already know the conclusion of that.

So we believe the way we're going to be configured as we move forward really increases our ability to execute in each business with the focus, and we're already seeing that today and I think you'll hear that in the presentations.

So to give a kind of recap, what did we see when we looked outside and thought about strategy? What we saw is security and information management are both exciting businesses but both are being disrupted and we're going to have a better opportunity to execute in those businesses if we stay focused, meaning two different organizations approaching that. So here's some of the key things that are different about security and information management.

Security is really being driven by the world of evolving threats. How do we provide more intelligence in real time? That means the pace there at which customers are willing to move is a lot faster. We just released our 20th Internet Security Threat Report. You can find that online, www.symantec.com/ISTR, and we'll talk a little bit about that later in Jeff's presentation, but no surprise to you, the landscape for threats continues to increase, not only in terms of number but severity. What does that mean if you're a security operations professional? You're frankly overwhelmed with alerts, more than you can take care of. We believe we have some products that you'll hear about, both Amit Mital and Balaji will talk about that—will help with this, so really looking at productivity. But for today, the world, these folks are really looking for help. They're screaming for help from us to not just provide another box or point solution; how do we help with a more comprehensive view of this problem?

The buying centers are different also between security and information management. So as security has become more important, as the budgets are increasing there, organizations are looking to CSO who sometimes reports to a Chief Risk Officer—not even the CIO in some cases—and then that person could even report to the CFO or the Audit Committee. As we all know, this has become very top of mind in boardrooms across the country. The need for the best solutions quickest means there are shorter selling cycles there. So, a great market but some very different dynamics than we find on the information management and storage side.

On that side of the business it's all about the exponential data growth. How am I not going to be swamped in the growth of more and more petabytes that need to be stored? The focus here is different though. The focus is not about how do I get the next quickest solution that's introduced in the marketplace? It really is about reliability and cost, and a key aspect of our portfolio, availability. So how do I make sure that that information can be backed up appropriately? How can we restore that?

That emphasis on cost and reliability means it's a different buying cycle. Those tend to be longer evaluation cycles, and here it is the CIO and the traditional IT organization that's still in charge of buying.

So two very exciting markets that we're in, but driven by very different things, which meant the synergy was not as great and the focus is what we believe is important for being successful in each of these markets.

So let's take a look at the strategy for each one of these which then is tailored to these dynamics and takes advantage of the unique assets we have at Symantec and Veritas.

Let's start with Veritas. John and Matt Cain, our Chief Product Officer, will be talking more about this. Just a quick highlight. The key in our Veritas business is the strength of the customer base that we've assembled over a long period of time. In fact, the average time I think of one of our customers to buy a product is six years. These are very sticky products. They really are critical. They're part of the critical infrastructure of these customers and that leads to the point on the right about scale. These are the largest, most complex organizations. Very large financial services institutions as an example, who would be interested in buying these products. In fact, while our market share would not indicate this. We believe we are backing up half of the world's enterprise data with NetBackup.

The hallmark for why customers turn to us, not only the reliability that we provide but heterogeneity. So if you're an IT buyer, you'd like to buy from someone whose product works across different vendors' platforms and in today's world that means operating systems, hardware, different clouds. You want to have that flexibility and Veritas has always provided that. That's kind of the heritage or hallmark of the Veritas product. So that's something that you'll see continue to be key as we look at the strategy of Veritas going forward.

This in fact is the strategy on one page, the product strategy for Veritas. Starting at the far left, it really is about continuing to provide the foundational products that customers continue to rely upon us to provide. These products really matter if you're in the IT organization. So these are backup, storage, business continuity. How do I recover from a disaster? How can I archive all of that information that's growing exponentially?

The challenge for us, and we believe we're prepared to meet it, is to provide that in a way customers want to buy it. So some customers want to continue to buy on-premise software. Others want to work with an integrated appliance; that's a much easier way to integrate this capability and maintain it a very low cost. As you no doubt already know, that's our fastest growing business within Veritas. And then we're increasingly moving to the cloud and what we envision is that there's going to be hybrid cloud. That's not everybody moving digitally from on-premise to cloud; they want to be able to work in a mixed environment. That's where the heterogeneity really helps us with our customers.

As we look forward, I'd say the two key planks of the strategy really are about up-leveling our capability so that we can combine the capabilities we've had in individual product to really give customers the ability to have more availability. Availability really is about movement of data. Even when data's at rest it's still moving as it goes to different tiers of storage and so forth. So a key part of the strategy for us going forward is availability in a world where that data is always moving. We'll be talking more about what does that mean. Then if you look over to the far right on Insight, how do you take advantage of the fact that because of backing up half of the world's enterprise data, what insight do we derive from understanding the data about that data, or metadata? We've been talking about a concept for a while, the information fabric, which really will help customers with this idea of insight, knowing what information, where it is, who's got access to it and so forth. We'll talk a bit more about what does that mean for customers, but pretty exciting new functionality that we're providing for the Veritas products.

The key advantage here is heterogeneity, as we talked about, and scale. So if we do our job right, that makes all of that information useful rather than being a slave to just how do I store all that information?

So let's shift from the information management or Veritas side of the business to Symantec. So we've talked in the past about Symantec's scale. Nothing really highlights the scale more than that bottom left. Nearly 4 trillion threats that we're monitoring in real time across the globe and that's updated at 200,000 a second. We don't believe anyone has anything close to this when people talk about looking for threat telemetry and the visibility that they have. So we often say we operate the world's largest bazillion (phon) threat intelligence network.

This is Symantec's key advantage but I can tell you I don't think we were taking advantage of this as we look in Symantec's history. We're now approaching a time when the tools for big data analytics can really be applied to this, and as many of you know, security is changing to focus on security analytics. So what if we could take all of that data

and make it useful for us to develop some real-time insights? You're going to hear a lot about that today because we are building that today. We are the only company, we believe, that has the combination of all of this data and the ability to take that and make it useful for customers to provide more secure outcomes.

So let's look at the Symantec strategy going forward. It starts in the middle here. We're building what we call a unified security analytics platform which really will take all of that worldwide threat telemetry and put it in a form that we can use it. The platform is obviously making that more usable so that we can search through that, look for anomalies, be able to say what are the differences in the patterns there that really are going to make a difference to stop attacks before they even start?

So this is all about not only using our own data but combining that with third parties. We have partnerships with some of the leading next generation firewalls, for example, to be able to use their data from the network and put this in the security analytics platform framework. We also envision a day when third parties might want to use this platform and write their own applications to it.

So with that as the foundation, if we look over to the left, the product portfolio is changing to be able to take advantage of that. On the Norton side, as Fran will talk about, it's really about simplifying the product line and getting one subscription service. We launched that last September and we love the traction we're seeing.

On the enterprise side of our business, it's really about simplifying what's 50-some point products and getting them focused around two different areas. Threat protection. This is a market that already exists out there and we have not been first to the party here but we believe we've got the best solution. That's because we're the only ones thinking about how do we look across all those control points, not just another appliance you can drop in, not just a next generation firewall that has capability, but how do I look across the environment and be able to see what are all the threats that are coming in, and then compare that to what we see globally? We're the only player that will have that capability.

The information protection side, we haven't talked about as much in our earnings calls but you're going to hear a lot about that today. This combines our DOP technology, encryption, identity and something we're calling user behavior analytics. That also will be benefiting from the unified security analytics platform. It really will be about keeping the good stuff in. The information we care about protecting, we've go great protection, which is a different part of the security problem than keeping threats out, and we think this is the next frontier in security and we want to be on it early.

Then we complement that by what you see at the right, services. Because many of our customers, certainly our smaller customers, don't have the security operations staff to be able to deal with the challenges in security and would like us to be doing more there. We're a leader in the services space today but we can be a lot bigger. It's a very growing, fragmented market and we are making investments to be a much bigger player there.

We introduced quite a few new services last year that went beyond monitoring to now incident response, threat intelligence and we'll be talking about simulation later today as well. This is supported by a very large global team of researchers and experts who are continuously scanning all of our data to see what's happening out there and making our product smarter.

So here are advantages about the global scale and real-time visibility, making that information more useful. Our belief is that if we seen more and analyze more, we can provide customers with more secure outcomes.

So let's shift now to how do we take advantage of this to grow? The keys to growing are we have a well-defined strategy; we've got the talent in place to make that happen, and we've got some very specific things here that we want to take advantage of to be able to grow. First, we in a rapidly growing market and some of the segments there are

growing much faster than 10%. So there's no problem and I'm sure everyone who walked in this morning had no concern that the market was going to be a limiter for us, and it's not.

What we've done this past year is shift that investment in R&D to growth market. We've increased the R&D dollars going forward and we've increased R&D as a percent of sales. You also know we improved our margins so how did we do that? Well, other functions had to shrink to be able to allow this but this is key for growth.

I won't spend time now because you're going to hear in great detail about the new products in the portfolio, but there are a lot more new products with enhanced functionality than what we brought to market in FY15. I'll let Balaji, Amit and Fran talk about that.

We've also improved our go to market. So while our total sales expense has come down from FY15 to '16, we increased the number of quota-carrying reps. We had a lot more overhead in the sales organization than we should have, so now there are 1,750 dedicated professionals who wake up every day selling security. Our sales organization before was not as focused. Folks were mixed in terms of what they might be selling, especially our international sales force. So completely dedicated. You're going to see the parallel dedication on the Veritas side.

Veritas is also addressing a growing market. We also shifted the R&D to focus on the new opportunities here that you're going to be hearing about today. So we're excited about new improvements to the foundational offerings as well as new functionality coming from availability and insight solutions.

Then similarly, an increase in the quota-carrying reps for Veritas and a very large dedicated sales staff which we believe is going to be key in terms of realizing the growth aspirations that we have.

So to sum up, we believe we can unlock significant value through the focus that we've already applied that now can lead to growth for the Company. So that's certainly what drove our expanded operating margin. That focus is what drove the investments that we made last year.

If you look over to the right, now what we want to do is leverage the scale. You saw for both Veritas and Symantec scale is a key part of our unique assets. Now we're going to drive some very differentiated product offerings that you're going to hear about.

On the Norton and Symantec side, we're the only company that's bringing together the scale of both consumer and enterprise on the security side, and now we're going to add the real-time visibility to that that will allow us to have both businesses be improving from a revenue compare standpoint. On the Veritas side, also a differentiated product approach is going to help us deliver some offerings in some areas that we believe are untapped sources of growth for availability and the insight solutions.

So I couldn't be more pleased—as I started this presentation—with the prospects. I hope you're going to feel that way at the end of the day. Let's continue as we dive in depth into the Veritas business. So it's my pleasure to introduce both John Gannon and the Chief Product Officer for the Veritas business, Matt Cain is with us here today.

As they come to the stage let me also introduce Brett Shirk who's our worldwide sales leader based here in the New York area, leading Veritas.

So, John?

John Gannon: Thanks, Michael. Good morning everybody. Matt and I couldn't be more pleased to have the opportunity to present you the Veritas business. I think you're going to discover that this is a very exciting business for now. We're experiencing accelerated growth as we exit the last fiscal year and enter this fiscal year, FY16. We're seeing expanding margins and significant improvement in our execution as well.

We have our presentation broken down into three segments. I'm going to first just talk a little bit about setting the foundation for you, so that you understand where we're coming from, the strength that we have to build upon as we enter into both the current market and expanding markets. Then Matt is going to spend time talking about the dynamics in the marketplace, kind of the steady-as-you-go dynamics as well as some of the new dynamics and expanding opportunities and adjacencies to what have been the typical information management marketplace. Then he'll go through our product strategy, talk to you very specifically about the product portfolio that we have put together; I think the most robust roadmap of products that we have had in many years in Veritas, in the information management business, that's going to help us both continue to meet and satisfy our existing customers and what they expect in our normal product portfolio as well as things they want to expand into and opportunities that they want to bring to them.

So let's talk now first about the foundation. So first of all, we have undoubtedly the most comprehensive information management portfolio of products in the industry today. These products are differentiated by—and have always been differentiated by the heterogeneous approach that we're taking to the marketplace. We play in the areas of information intelligence, information availability, backup and recovery and of course now our integrated backup appliance product. Customers want and appreciate the heterogeneity of our product portfolio, and as Michael talked about, as their infrastructures build out and they have more and more platforms, virtualization, et cetera, that they're trying to deal with.

Now we take that product portfolio and we apply it to what we believe is a very exciting and steadily growing market, growing at 7%, to 2018 reaching about $18 billion. But in addition to that, we see and analysts see perhaps even larger numbers than we're attributing and the incremental $6 billion worth of available market in such areas as software—recovery as a service, software data management and copy data management. These are areas that we have new products that we'll be introducing this year which Matt will spend some time talking about.

Then—I'm sorry. Could we back that up one? Thanks.

So with these products, with the marketplace, we also have the exciting position of being in product leadership positions. In each of those four segments that I talked about, we have either number one or number two market share positions. Our appliance product is the fastest growing product in the industry. I'll spend some time and give you just a little more detail on that in just a moment.

We have sustained market leadership positions in Gartner's Magic Quadrant in a number of areas for many years, in the area of archiving, e-Discovery and backup and recovery.

Mike alluded to this but on top of it all, we have the most enviable customer base I think in the industry today. We're pleased to have over 86% of the Fortune 500 companies as our customers. This amounts to over 50,000 enterprise customers, and as Michael alluded to, not only is this a large and broad customer base but it's a very loyal customer base. We have over 6% retention of these customers for over six years. Likewise, the majority of these customers have been with us for over 10 years; so six years average, 10 years for most of the customers.

Okay, now this brings us into the strong business momentum that we're seeing coming out of FY15 into FY16. First of all, let's talk about growth. We began the year at 0% growth, which was significant improvement coming off of a negative 4% in the quarter before in the previous year. So even 0% was significant improvement, but that momentum now has continued through the year with 3% growth in the second quarter and 5% growth in the third quarter. We believe that this acceleration is going to continue. We can see the way to it, the path to it into FY16 and into FY17.

Now this growth has been aided significantly by the success we've had with our backup appliance product, which once again carries with it our NetBackup software, the industry-leading backup software. We have seen between calendar year '13 and calendar year '14, which is the way the industry analysts look at it, a 20% increase in that product, which is nearly five times the industry growth rate of 4%. Now hidden in these numbers is another very unique number and that is at this point we believe that we are only 10% penetrated into our customer base with these backup appliance products. So we have 90% of our customer base to try to upsell to as we go forward. In addition to that, of that 10%, somewhere between 40 and 50% have made repeat purchases of the appliance. So not only have they bought their first appliance but they have bought multiple appliances. So when you take the 90% upsell opportunity and think about multiple sales into that customer base, we think that really bodes well for the growth of this product line going forward.

Now we have been making significant investments for some time now in our product development process, moving from a waterfall approach to developing products to an agile methodology and we already have seen very significant benefits from that in two areas. The first area is in the velocity with which we're able to bring both new products and proliferation and maintenance releases to the marketplace, and secondly in the area of quality. The code quality of our products that we're bringing to market has significantly enhanced.

Just to talk about the efficiency part of it for one moment, it has in the past typically taken us about 270 days to bring a proliferation release to the market. We have reduced that now to under 70 days. What does this efficiency mean? It means two things really. Number one, it gives us the opportunity to bring more products, more releases to the marketplace in the same time, and secondly it gives us the opportunity to free up resources to apply to some of these expanding market opportunities.

Lastly, while we've been going through the separation process, we've had the opportunity to really focus on our organization, focus on the efficiency of the organization. We've done I think great things with our product organization, adding to that under Matt, Chief Technology Officer, that can be focused on enabling technologies, unique IP and help us ensure that we have that going across each of our products to avoid repetition and to avoid doing duplicative efforts in different areas.

We have a worldwide dedicated sales organization which I'll talk just a little bit about in a second. Likewise, we have moved from a siloed support organization to a worldwide customer support organization and we're seeing benefits from that.

Okay. So the focus for us is driving results. In the first instance, as Mike mentioned, a 20% improvement in the number of quota-carrying sales reps that we have in the organization. Secondly, while doing that, Brett has been able to sign up for a 25% expense to revenue ratio which really is coming down, bringing us back in line with what we perceive as being the industry standards.

I talked about quality. The two pieces that are enhancing our quality really are number one, the agile development process, and number two, the support that we're able to provide our customers with this focused worldwide organization. We now are enjoying over 90% customer satisfaction. In fact, it's my understanding that in this last quarter, our enterprise customer support satisfaction exceeded 95%. We're likewise seeing improvements in our partner customer satisfaction; extremely important to us as over 70% of our business is in some way touched or enabled by our partners. So their satisfaction with us is critical to our success going forward.

Then lastly, we talked about the margin improvement and Thomas will give you a lot more color on this in his presentation. But between Q1 and Q3 of FY15, we've seen 12 percentage points improvements in the margin. We also can see our way very clearly to continued improvements in margin as we enter into FY16.

So that's the foundation. I'd like to take a few minutes now and introduce Matt Cain to do the balance of the presentation. Matt joined Symantec Veritas about three years ago after distinguished contributions at Cisco. Matt had the opportunity to start and launch our integrated backup appliance product, putting together what I think is one of the most competitive business models in the industry for both delivery and support for the product.

So with that, I'd like to introduce Matt.

Matt Cain: Thank you. Well good morning everybody. It's great to be here. As John mentioned, I'm going to cover two primary topics over the course of the next few minutes. The first is about our market and in that I'm going to talk through some of the trends and challenges that our customers are facing and then put some numbers behind it. Then the second part of the presentation is all about our product strategy. I'll start with our philosophy around availability and insight, and build up to our five-quarter roadmap where we get into specific releases and our cadence. So let's jump into it.

As Mike mentioned, data continues to grow at an exceptional rate. As matter of fact, when we sit with our customers around the world, they always try to forecast how much their data is going to grow in the following year and usually they've come in somewhere around 40 to 60%, and every year they're wrong, being on the low side. As a matter of fact, by 2020 it's predicted there's going to be about 44 zettabytes of data around the world. You might ask yourself what does that mean. Well today, there's around 4.5 zettabytes. So based on all the data and explosion we've seen with things like the Internet of Things, new applications, we're going to see an additional 10-fold increase in worldwide data. So what are our customers going to do about that?

The current approach is to throw infrastructure at the problem. This is next generation storage, software defined networking, cloud technologies, virtualization, and companies have the hypothesis that if they continue to invest in bigger, better, faster, they're going to achieve business agility while managing all this data, but we don't think that's going to work.

If you look at the realities within an IT organization, both from a budget and a resource perspective, the growth rates of data are simply bigger than what IT organizations can afford. Sixty-two percent of all IT budgets are spent just on maintaining existing infrastructure. So our CIOs, before they get even out of bed in the morning, two-thirds of their budget is gone with no ability to invest in additional infrastructure, or certainly not to change their approach. So if they don't have money, what about people? Can they throw people at the problem? Well actually IT budgets, according to our information, half of them are going down, not increasing. So what does that mean?

What it means is you need a different approach and that approach is about managing at the information layer. If you look at some of the dynamics that are happening around our customer base. It's predicted by Gartner that 25% of companies are going to have a new C level role just focused on information; they're calling that the Chief Data Officer, and it's one example of organizations trying to get their hands around this concept of managing information.

Now that's not a new perspective for Symantec and Veritas. In fact if you go back to the beginning of our company, we've been focused at the information layer from the outset, and our approach is not just to be at that layer but it's to do it heterogeneously across different storage arrays, across different operating systems; as new applications emerge, ensuring that we are helping our customers so that they can deploy those and remain confident with our underlying software.

Now what about the dynamic of cloud? Our customers certainly want to take advantage of cloud because of the flexibility that it offers. At the same time, they don't want to lose the control that they enjoy around their information. They want to have visibility. They want to be able to manage it. They want to be able to sleep at night knowing that their applications are going to run in these changing environments, as Mike talked to. And just like we've helped

companies through the transition from tape to disk, we're well-poised to help customers with the transition from premise to cloud, particularly in a hybrid cloud world, and I'll go through how we're going to do that with our portfolio.

So these are some dynamics around our foundational opportunities. Let's shift and look at what it means going forward.

So with that focus on information—I'm sorry, on infrastructure and the explosion of information with new technologies, clouds, et cetera, we have this concept that we call fragmentation. If you think about all of us in the room, we're sitting here with laptops and mobile devices and tablets, and on each one of those there's different information; different information that we're creating; different information that we're moving; different information that we're drawing upon from different storage repositories. Now imagine how challenging it is for a CIO to have visibility into that information, let alone manage it and provide the level of SLAs that we all demand as business users. When you start to take this to next generation applications and the complexities of our worldwide customers that presents availability challenges that cannot be solved with today's solutions.

So what are companies doing? They're trying to respond to this by coming up with new ways by throwing money at new solutions big data. A hundred and twenty-five billion dollars is going to be spent this year alone on big data projects, and that's all about trying to get a handle on this information; somewhat of a unique approach to understanding information and give some insights into it.

What are those companies really after? They're after the needle in the haystack, as we call it; that is the valuable information that if they had access to it when they needed it they could make better business decisions. And it's a very small subset of that data when you look at the entirety of it, about 1.5%, that is truly what we call target-rich; if you had it when you needed it you could make business-impacting decisions.

Now, more evidence that companies are trying to throw people at this problem, according to LinkedIn in 2015, the hottest job that got people hired was that of a data scientist. So they're bringing in people and saying, "Look across my information and try to put some sense to this to help us be more competitive. Give us that edge that we need based on the information we have." McKinsey's onto this thread as well, but they predict by 2018 there's not only going to be a shortage of these types of people, there's going to be a shortage of over a quarter of a million of those types of people because, again, the pace of data growth is just faster than we can keep up with.

So what's another way to get at that needle in the haystack? Well, as we analyze the 1.5% that could truly enable better business decisions, it turns out that over half of it exists in what we call general IT metadata, and that's the information that we as Veritas already touch, and we touch it at an exceptional level of granularity. Mike talked about the business that we're in, primarily around backup, so being able to restore a single file at any instant to a user around the world. Imagine how much information you need to collect and catalog and manage to be able to perform that job. Same holds true for archive and storage management and availability, and we have access to all this metadata but we've been primarily putting it to use to do our core job, those core jobs that I mentioned.

So as we go forward, our plan around insight is to continue to amass this data because we have world-class availability solutions, but start to put it together in a way that we can unlock that value, to get at that needle in the haystack. To give you one example, it's widely recognized that today about 70% of the data that's stored in enterprises is completely useless: no business value, no value around compliance; you don't need it for litigation. In fact it can be even more challenging to keep it from that perspective, and yet we keep it forever. If you've been approached by your IT department and they say, "I'd like to delete your email," you say, "No, don't delete my email," even though we never go look at an email that's six months or certainly not seven years old. But companies need the confidence to delete it and imagine how much resource they could free up if we just allowed them to get at that 70%, and that's just one example of the business insight that we're talking about.

So let's put some numbers behind this. John talked about our foundational product total addressable market and in calendar year 2013 that added up to about $12 billion, and you can see the breakdown by the products that we cover. The growth rate is just over 7% compound annual from 2013 to 2018, so that's going to increase our total addressable market over the foreseeable future to $18 billion.

Now, when we start to go beyond those foundational products and extend our portfolio, as both Mike and John alluded to. We have next generation opportunities that very conservatively add another $6 billion to our TAM. Those are in areas around copy data management, recovery as a service, software-defined storage.

When we say conservative, we sit with market analysts a lot, share what we're doing and get input, and when we talked about our roadmap which you're going to see in a moment, they said, "Six billion dollars, that's crazy. That could be five or 10 times the size." So the way I think about this is whether it's $6 billion or $60 billion, we are not opportunity-constrained and our ability to execute in this amounts to a doubling of our total addressable market. So while many of you may have walked in here and thought that security was not constrained, to Mike's point, we feel equally strong about the opportunity in the core markets that we're in as well as these adjacent markets that are very close to the technology that we have, very close to the install basis we have, and we believe we're very well poised to take advantage of this.

So let's shift gears to our strategy. I mentioned that we've been in the information management business for some time and over the last several decades we've learned a lot, and a big part of how we think about our next generation opportunities is by sitting with our customers and saying, "How can we better meet your needs? What challenges are out there that technology doesn't have a solution for?" When we put those two things together, we know for certain that to have a comprehensive information management strategy you need two things. The first is you have to have information availability, having what you need, when you need it, wherever it resides. But the second, based on the trends that I talk about, is you have to have information insight. Knowing what you have, leveraging what you know to make better decisions, and this is really what's driven our philosophy around availability and insight that's going to push us to innovate in these areas and the combination between those as we go forward.

So where does it start? It's starts with the foundation, and our foundational products around backup and recovery and storage management and disaster recovery and archiving, these are fundamental solutions for our customers today. They depend on it. John and I have been in New York for the week. We've been going around talking to major customers here and the tell us how critical these solutions are. They ask us to continue to work alongside of them because of how dependent they are on our solutions as they move forward with their infrastructures. So we're going to continue to innovate and build solutions for hybrid cloud deployments across our foundational portfolio.

At the same time, they're foundational for us, certainly from a business model but also as we build out our next generation solutions because none of our next generation solutions are we stepping out and saying, "We're going to go write unique code." We are leveraging our technology. We're taking advantage of the capabilities that we have in our working software as well as the information that we have and the install base that we have. In a lot of cases we're able to come out with next generation solutions without any impact to production environments which other companies that are trying to insert themselves into these areas don't enjoy that advantage and it creates challenges for customers. So the foundation is paramount to how we go forward.

Now let's talk a little bit about some of the next generation solutions and I'm going to give you very high level preview of four, all of which will be out within the next year.

Veritas Velocity is the first one that I'll talk about in the availability side of the business, and that is instant self-service access to secured instances of copy data, again with zero impact to production. So these are all the evolution of how we do backup into next generation data management leveraging data virtualization technologies, streamlining the amount of copy data that's required to open up new use cases and still protect the information that our customers need.

The second one is what we call the Veritas Resiliency platform. This is a business continuity software solution that provides application level recovery. So imagine if an administrator had an application running on a data center in New Jersey with a set of operating systems and infrastructure and he or she wanted to move that application to a data center in Santa Clara. With a simple click and our software, understanding the underlying infrastructure, they could move that very seamlessly for disaster recovery purposes or to update the infrastructure here in New Jersey, and the flexibility that that provides in our fast-changing environments of our customers is what we're proud to be releasing and what customers are asking for.

As we shift to the information map, this is a simple cloud-based tool that provides end-to-end visibility of a customer's information, and in a minute I'll show you what that looks like and then highlight a few more points.

Then the final one is retention management. As Mike talked about, our next generation solutions is about integrating our capabilities and providing automation and better workflows and easier experiences for our customers and this is one example where we will expand beyond traditional archive and leverage things like file classification to build a more robust product suite.

Now, as we deliver on these, we're very focused on architectural differentiation; architectural differentiation not just to create sustained differentiation for us but to help our customers bring technology together, and we have two distinct architectures: one around the availability suite which we call information orchestration. This is all about how you move data, how do you understand it, how do you do so in and between clouds from private to cloud, and across our solutions we're going to be doing that but we can combine the IP to do it efficiently on behalf of our customers.

The second is a concept, as Mike said, that we've been talking about for some time and that is the information fabric. The information fabric is the architecture where we're going to stitch together all of this metadata, and that's metadata that we're going to pull from our own data repositories like our backup catalog and our archive, but we've also architected this for cloud and an open infrastructure that we can pull in other metadata like Box or SharePoint, things like that so customers can have one coordinated architecture for all of their metadata and true visibility across the entirety of their information landscape.

So what I want to do is show you a quick video, and this video is going to highlight some of the business challenges that I started off with, and it's going to start to translate how we're taking some of those challenges and building them into two of the four next generation solutions that I talked about that are going to be coming out in the next six months. Both of these are in beta with several customers. As a matter of fact we're probably oversubscribed based on the demand, but you can start to see the level that we are going up the value chain and the simplicity that we're building into these technologies. Let's roll.

(Video presentation)

Matt Cain: So hopefully you get a feel for the level of simplicity that we've built into these user experiences, and while that highlights two of the next generation solutions, again keep in mind how dependent those are on our foundational products and our customers continuing to enjoy the benefits of those as we add these layers on top.

Now I'm going to talk through the product roadmap and give you a sense of those 17 products that Mike talked about: 14 foundational and three next generation. Before I do that I want to take a moment to give you my perspective on the Agile transformation.

This is one of the initiatives that we took on as a company and somewhere between 18 and 24 months ago it was a massive overhaul of how we do development. On the Veritas side of the business about 80% of our engineering teams are now fully functioning in Agile methodologies, and this not only adds to the pace at which we bring solutions out but equally if not more importantly, it's the velocity of features that are in each one of those releases, the predictability of the releases themselves and the quality that we're delivering them on.

The roadmap I'm going to show you is the healthiest it's ever been and the confidence that we have in it is the highest we've ever had because of how these releases are tracking and the measurements that we're taking along the way. And in each one of these you'll see that we have major releases across every one of our core products, and while we're excited about the concept of availability and insight in the next generation solutions, each one of these product releases have differentiated features that are well positioned to take advantage of our core markets.

So let's start with the first column, business continuity and storage management. You'll notice the blue releases are all about foundational and that goes after the 12 growing to $18 billion total addressable market. So within business continuity, some dynamics that are happening in this business are hardware commoditization, next generation storage technologies, the need for disaster recovery and better SLA management, and we want to take advantage of all of those, when we first talk about the storage management part of our business. Software-defined storage is a term that we're all hearing and what does that really mean? Customers want more flexibility in how they're deploying next generation storage technologies, either further commoditizing traditional arrays where they're not deriving the same amount of value, or investing in next generation technologies like solid state arrays, and they want to deploy the right set of infrastructure for the right applications. The more expensive high performing ones they don't need for every application. So where they're using our technology they're saying, "Well you guys have always managed across storage environments. Now I can deploy these storage technologies but still enjoy the benefits of one single management console where I can ensure that I'm deriving the efficiencies that I'm looking for and the benefits of new storage technologies." Making sure that it's still completely up and running to meet their needs.

On the business continuity side, we're overlaying solutions around disaster recovery. This is all about ensuring that we have application level awareness. See, a lot of the infrastructure approach is let me build as many nines of reliability as I can at the infrastructure layer, but CIOs, we actually met with one this week that said, "I want to be able to sleep at night." Where they get that sense of confidence is not just focusing on ensuring that you have your environment and that it's built as it moves, but you have that overlay of insurance looking at the application. So each of these releases are focused on software-defined storage flexibility as well as that business continuity.

Shifting over to backup and recovery. Our philosophy on backup and recovery starts with our software and that is to build one integrated platform that can back up a customer's entire environment with flexibility at the application layer, multiple databases, every operating system, hypervisor and then freedom of choice with secondary storage, and we're going to continue to innovate along that value proposition with a lot of focus on enabling cloud-based targets and self-service access for more cloud-based deployments for both enterprise and our large partners.

Within the appliance form factor, our focus there and our strategy has always been about the customer experience and what's customers asked us to do is they said, "We love your recovery software but I still have to put that on infrastructure and then I have to choose storage. Can you build an integrated solution for me that helps me deploy and consume your software but does it in the easiest possible way for me?" That's what we did with appliances and that's why we're seeing the growth that we are.

Now that we have the foundation that we've built up over the last few years, it's all about adding capacity and the performance to go with it. So what this represents in the quarter that we are in now, we're now shipping an appliance that's almost 230 terabytes and in the back half of the year, we'll scale that again to over 460 terabytes, and while we'll talk a lot about the capacity, we're equally excited about the performance that goes along with that, being able to get data in and data out to meet customers' backup windows and the demands of their overall environment.

So we shift over to our eDiscovery and archive portfolio. A couple of things we're focused on here; the first is scale. So as data continues to grow, so too do the demands of the archive itself and the eDiscovery technology that sits on top of that, and so we'll continue to build that out for more and more users and more and more data. We also want to focus on other data repositories, things like ensuring that our archive is streamlined to work with Office 365, ensuring that we can provide file classification from repositories like Box and continuing to build up the core technology around insights that will feed the rest of our portfolio.

Then in the next generation solutions which I've covered, you can see how the releases map over the next five quarters. I mentioned that there were three releases next generation this fiscal year. You probably are counting four. This isn't a matter of under-committing and over-delivering; it's actually that our Veritas Resiliency Platform, that business continuity solution, comes in two flavors: one that we will sell directly to customers and one that we have aligned with HP to take advantage of their services and their cloud capability with our software fueling that solution. We've issued a press release on that in the last couple of months that you can take a look at.

Then around insight, it's all about the information map and delivering on that, proving to customers that they do have investment protection, first with NetBackup and then continuing to add new sources of metadata that will only increase our visibility and then help us move to management and control with things like Retention Manager and other applications that will build on top of the information fabric.

So what are our customers telling us about this and what does it mean for growth? Here's two examples of quotes from our CIOs, letting us know that they're aligned to seeing us as an information broker. One customer has talked about, "I've been in this business for two and a half decades. I've been throwing infrastructure problems. I've been spending billions on it, but now I'll finally know if I'm being successful and if I need to do something different." So we think there's exceptional growth with our product portfolio and our strategy going forward.

So John alluded to the focus that we're deriving with breadth and the go-to-market organization and we see additional uplift to our business, leveraging some of the initiatives that Mike and Thomas have alluded to as well, things like how do we change our pricing models to better meet the buying demands of our customers, things like capacity-based pricing models which we have in certain parts of our portfolio but not all of them, getting more diligent and disciplined about how we're managing discounts or monitoring license compliance and focusing on the customer experience. John talked about our customer satisfaction scores. We are very much of the belief that we'll continue to invest in the right levels of support, and we will continue to increase our overall customer experience, which is only going to raise maintenance renewal rates.

So with that, let me close on the slide that Mike started with. We talked about our investment which we are increasing year-over-year from an R&D perspective in Veritas like we are in security. There are three aspects to our investment plan; that of foundational products but also delivering availability and insight and pulling these together with coordinated architectures like we haven't before. We'll continue to be very focused on heterogeneity because that's what our customers are asking for and, ultimately, want to make every byte of data actionable for our customers.

So with that, let me turn it back to John.

John Gannon: Thanks a lot, Matt. If it hasn't come through yet, we're pretty bullish about the Veritas business. Also, if it hasn't come across, we are really all about accelerating growth, about expanding margins and about improving our execution. These are just a few of the bullet points that we've already gone over today. I probably don't need to reiterate them, but thank you very much for the opportunity to present to you, and I think we have a few minutes left for questions.

Helyn Corcos: So we're going to pass mics around. Sean, go ahead and take the first question. Thank you.

Aaron Schwartz: Hi, good morning. Aaron Schwartz with Macquarie.

John Gannon: Morning.

Aaron Schwartz: Thank you very much. I had two quick questions. First on the last chart you had here, the portfolio growth drivers, most of these seem very operational focused, not really on the new product side, so what would the timing be for you to release the incremental growth from all the new products you introduced?

Then secondly, I didn't hear one mention of Backup Exec. I know that's been a problem product for you. Can you just give us the status of the commitment to Backup Exec? I think last time you disclosed, that was about a $400 million product. Can you just update us on where that is? Thanks.

John Gannon: Okay, so let's take those in parts. So the drivers on the growth beyond the product, those are ongoing and I want to make clear that we're investing in product to enable those. There aren't—those aren't just business models, so making sure we have the telemetry to take advantage of things like capacity upgrades and what customers are using, so we think we'll only continue to benefit from those initiatives. In terms of driving growth from our portfolio, we do have forecasts aligned to our next generation products this fiscal year, so as we release, we're not certainly expecting to derive new business from those.

Your question on Backup Exec, we remain committed to that. We're not expecting to grow that business like we are other parts of our portfolio, but as evidenced by the fact that we just had a major release in the last month, which we call BE2015 which helps customers with hybrid cloud deployments in SMB. On top of that, we're also continuing to invest on the support side. So we're focused on doing right by our partners and customers in that space. It's an important business for us, but it's not one that we're expecting to grow.

Walter Pritchard: Hi. Walter Pritchard at Citi. On the cloud side, you talked about supporting people backing up however they want to back it up, but I think when there were some management changes at Symantec, one of the product areas that was sort of stepped back from was some of the dot cloud initiatives and I'm wondering what your approach is in the cloud. Is it connecting into third party sort of targets that you could back up to? Is it building your own capacity? How does that look and—because we hear that a lot in terms of SMBs moving to the cloud for backup. It may be inevitable in the enterprise market as well.

Matt Cain: So our approach to cloud somewhat varies by the different business we're in because the dynamics can shift between business continuity, our archiving by cloud product and backup. Specific to backup, we certainly want to enable the flexibility of customers getting their secondary data into cloud storage repositories, and we're investing in both our backup and recovery software on both the enterprise and the SMB, as well as our appliances and making that efficient, but customers want to move it, they also want to keep it in our catalog so they can recover it when they want to. So a lot of that is about enabling the hybrid cloud with respect to backup and our customers are taking advantage of that today. That's not a new thing.

At the same time, we want to help them in how they deploy and manage backup, so this is about backup administrators being able to configure and administrate backup solutions with more flexibility. and that's when we talk about self service and some of the multi-tenancy that we've put in. In other parts of our portfolio, John mentioned the creation of our CTO; we are standing up cloud capabilities, where, if customers want, we will run it and manage it on cloud infrastructure that we would brand as Veritas. Certainly a good example of that would be our cloud-based archiving product, and there are other subtleties across the portfolio. But I think we're where we want to be with respect to cloud, the flexibility and the enablement across our customer base.

And I should mention, all of our next generation solutions are cloud first, so every one of those will be deployed in the cloud and we're not starting from premise and then evolving to that.

Keith Weiss: So Matt, I thank you for the presentation. This is Keith Weiss from Morgan Stanley. A lot of new appliance and a lot more capacity in appliance is in the product roadmap. Can you talk to us a little bit about what kind of uplift you guys see—when you go into a traditional Veritas software, like a NetBackup software customer, then you're able to sell them the underlying infrastructure and underlying storage? Can you help us quantify what kind of uplift you see and maybe how far into the days do you think you are in terms of selling these appliances? What percentage of your customers have taken on the appliance form factor? How much more room do we have to go in that regard?

Matt Cain: So I'll talk about the dynamics and then, John, if you want to pile on. I showed the different capacity points. If you look at the bulk of the success we've had and the numbers that John alluded to and Thomas will show, keep in mind that the majority of that has been delivered at 76 or maybe 140 terabytes of capacity, and with that form factor, we've gone to customers and said, "For these use cases, we have a solution. If you want to scale, we're not the right provider for you." The solutions that we've delivered at this point have been about remote offices and where we're combining software and underlying infrastructure, and with that, we've penetrated around 10% of our customer base. So what that means is a NetBackup customer has bought an appliance. But to John's earlier point, in the last quarter, around 40 to 50% of our business was customers buying new appliances. So the way this typically works is, will I buy off on the value proposition? Let me put one in my lab and let me move one into production and see how it goes, and the fact that that trend has continued to increase proves to us that we've got the value proposition right.

Now as we add the additional capacity points, those conversations of, "Well, we can't play in this particular," are over, particularly when we get to the back half of the year, and the customers that we were seeing this week, as you can imagine, have some of the largest infrastructures that we've seen. They're quickly moving past evaluation into production with our appliances and whether they fall on the side of having already purchased one, the forecasts within those are exceptional. So too is the forecast to get after the rest of the 90%. So we think there's tremendous opportunity to continue to scale our appliances, and we're very excited about the fact that we have the foundation of customer experience, everything from manufacturing and supply chain and our 24x7 secure operations center that manages that base to alert customers if there's a problem. So there's huge upside and it's driven because we've responded with a unique value proposition that no one else in the industry has, where we're combining that single platform with the underlying infrastructure.

John Gannon: The only thing that I'd add to that is uniquely for ease of integration for the customer, these customers are already NetBackup customers of ours, so they're now integrating an appliance which is supportive of the environment that they already are very familiar with and well established.

Keith Weiss: Can you (inaudible) sense of just like a percentage uplift you get from a customer?

John Gannon: The percentage uplift from when we add the appliance?

Keith Weiss: Right, and a Veritas customer that is paying you $100,000 for the software, if they're not going to be buying the appliance, what type of percentage, although (cross talking)?

John Gannon: Yes, we don't really evaluate it that way. We track our appliance in a hardware-only perspective, and then we track the software—the NetBackup software that's integrated with it, we track that in our software numbers, so we don't differentiate between the two.

Matt Cain: So it is additive. I don't know that we're prepared to go to the level of granularity that you may be looking on software attach rates, but I can tell you it's not cannibalizing. It's all additive.

John Gannon: Yes.

Matt Cain: Yes.

Keith Weiss: (Inaudible). Trying to figure out what the percentage (inaudible).

Matt Cain: Yes. So I don't know if we're going to break that down later.

John Gannon: I don't think we will be.

Matt Cain: Okay, yes.

Helyn Corcos: We have time for one more question.

Matt Cain: There's one over here.

John Gannon: One over here.

Male Speaker: Thanks very much for making the effort. However, two (inaudible) fairly small product questions, I guess. One, you mentioned copy data management. Can you drill down a little bit more on that product and the roadmap for it? Also, you didn't talk much about backing up and protecting on arrays; in other words, snapshot-based management, how much you're seeing that as an area that people need—some people need to do and what you're doing there.

Matt Cain: So let me start with the second and then I'll get back to the first part of the question. In terms of array-based managements, snapshots, that's a technology that we've invested in for quite some time. So we have a technology that we call Replication Director, where customers can still enjoy the advantages of snapshots between arrays, but then we then use one of those snapshots to catalog the data, which gives them the next level of protection if they want to recover at an individual file level. Because snapshots work theoretically but if you want to recover to the level of granularity that our customers expect, that's where it breaks down, and we're working with several storage partners on that balanced approach, where customers take advantage of the snapshot but we still build it into our catalog.

As far as our copy data management solution goes, first I would say that we're not approaching this as let's go build a me-too copy data management solution. The way we look at this is an evolution to how we do backup. But what customers are asking for is better orchestration technologies where once they back that up, first of all, can they do that more efficiently where they're not adding to the problem of the 70% of data that's useless, and a lot of that is copy data, so how do we help shrink that down and how we perform backup? But then how do I open up new use cases for customers where I can orchestrate the movement of production level data, having masked it, and send it things like big data repositories where you want to run real time analytics on all the data that we touch? Or let's say that you want to move that over to a test and (inaudible) environment where companies are rolling out new technologies and they want to see how those new technologies would perform on their production level data. So we're taking our approach about orchestration. Implicit in that is better copy data management and data virtualization, but we're going to take a unique approach again that builds on our backup foundation.

Helyn Corcos: Thank you so much, John and Matt.

John Gannon: Thanks.

Helyn Corcos: We are ready for our 10-minute break. Thank you so much.

So before I introduce the next speaker, I just wanted to give just a quick kind of a plug for an option that we're going to have for you during our reception time. Of course, you'll have lots of face time with the executives during that period. We are also offering three demonstrations of security products that we will be discussing a little bit later in the presentation, so you might want to think about whether or not you want to sign up for one of those three demos or to be in a group to see the demos. So I'll give you that food for thought and we'll have signup sheets out by the registration tables during the lunch time.

At this time, I'd love to introduce our Head of the Consumer Security Unit, and, Fran, come on up.

Fran Rosch: Thanks. Good morning everybody. As Mike said, I'm sort of the veteran of the Management Team. As a bit of background, I joined Symantec about five years ago as part of the acquisition of the security division of the VeriSign, of VeriSign. Spent about my first three years in the Company integrating the certificate authentication businesses into the Company and happy to report they continue to still do well. Spent about a year on the enterprise product side and then about a year ago, as Mike came on, he asked me to take over as the General Manager of the Norton business. Had a great FY15, happy to give you a quick update on that and then talk to you about what we see for the future of Norton in FY16 and '17.

So just as a quick agenda, talk with you about our business priorities that we focused on in '15 and continue to work on in FY16. Then take a quick step back, talk about the threat landscape and the market from an external perspective and then sort of give a state of how we're doing against those, and then really spend the bulk of our time focusing on our growth initiatives, as well as taking the time for Q&A at the back end.

So when we look at FY15, we really had two big priorities as an organization. The first one, which we really consider complete, was to focus on improving those operating margins. So as Mike talked about, we improved those by over a thousand basis points to 53% and were successful in generating a lot of cash that we can use to invest into the enterprise security growth opportunities that Mike talked about and you'll hear a lot more from the enterprise team after I've completed.

So our second big focus was on revenue; how do we work to mitigate that revenue decline that's been going on now for several years? We focused that in two core areas, one around the product and one around the go-to-market. In the product, we're focusing on a much more simple services for our customers, shifting them from a product billing model to a subscription service, and then focus on improving the end-to-end customer experience. We believe those will help us mitigate that revenue decline. From the go-to-market perspective, we're really increasing focus and our experience around digital marketing and digital acquisitions and communicating to our customers online. That has the benefits of higher ASPs with our customers, as well as they tend to stay with us for many more years.

So I'm going to spend the bulk of the presentation focusing on those revenue initiatives, but I want to take a quick look at the market. From the Norton standpoint, we have a very important mission in keeping our 63 million users safe and secure, and that becomes more challenging every year as this threat landscape continues to become more sophisticated, so I'll just hit a couple of these spots. One point there in the upper left is just the increase in the amount of unique malware of 26% to about 317 million last year. The reason that's important, those are unique variances of malware which cannot be caught with signature-based antivirus protection. These require the advanced layer of security that we built into Norton over the years around behavioral analysis, reputation-based to catch those sophisticated threats.

Another thing you probably read a lot about is ransomware or online extortion, where the bad guys are able to get on consumers' PCs, lock up their information and actually extort money before they'll let that go. That's a very intrusive type of attack and really causes consumers to look to the best security to keep them protected from those types of advanced attacks.

Finally, I think over the years, we've trained consumers better not to click on emails they don't recognize or suspicious links, so the bad guys are starting to get around those guys by actually embedding their malware into software that is legitimate, that we do click in and download, allowing that code to get on the PCs and cause problems for our consumers. So this threat landscape's continuing to get much worse for our customers and it requires much more sophisticated technology to protect from that we've built into Norton and certainly most freeware suppliers don't have, as well as many of our competitors.

So when we go ahead and look at the actual market then, you heard a lot about a fast-growing information management market and you'll hear about a fast-growing enterprise security market. The consumer PC security market is growing much more slowly. We estimate around 2%, so it's a slow growing market. However, from the Norton standpoint, we still have the bulk of around 43% of that paid security market, so we're still the largest player by far, more than twice our closest competitor. As I mentioned, we have a great foundation in the Norton business. We protect 63 million customers, primarily consumers that are paying for that service, but as well as about four million small businesses that also feel comfortable with the Norton brand and the protection that we provide for their businesses.

Part of the reason that Norton can be so effective in keeping our customers safe is we leverage the telemetry, not only from the 63 million consumers but the broader 175 million endpoints that we as a company protect across both the Norton and the security brands. We also spend a fair amount of our marketing dollars primarily in acquisition and retention but also continuing to ensure that our brand stays number one. We constantly survey that and the brand continues to be number one in innovation, number one in protection in most of the markets around the world. So it's a very good foundation that we have in the Norton business from both a technology as well as a market perspective as we continue to focus on this core market of PC security.

But as we all know, consumers are really moving beyond the PC and moving into the mobile space, and that continues to be an important market for Norton as well; however, it's quite different. It's much, much smaller. From a dollar standpoint, we predict that the mobile market is less than 5% the size of that PC security market, and the reason for that is most customers are satisfied with the free services that are out there, the types of threats have yet to really grow significant on those mobile devices. So most of the mobile security out there is free, about 85%, and even the 15% that is paid has a much lower ASP. So overall, the market for mobile is much smaller.

However, it's a very important part of the Norton strategy and where we continue to make investments. We actually just recently won an award at Mobile World Congress for innovation around mobility products as we look to develop what we call our Application Insight. Where the operating systems for mobile are more secure, a lot of the applications are not. Many of them are malicious or just grayware and cause a lot of problems for consumers, so we've released some innovative technology that allows consumers to actually gain more insights into how those applications will perform in their devices.

From a security standpoint, we really break our mobile security strategy into four different pieces. First, we recognize that our consumers are all part of multi-device households, their multi-device lives. They have PCs, Macs, mobile, so everything we do from the Norton perspective now is multi-OS, multi-device, so we've integrated our mobile capability into that core Norton subscription service. That really helps protect our customers, helps increase our retention rates.

We also believe that our Norton mobile security is also an introduction of the Norton brand to a new generation of Norton customers. Many people who start out with Android or iOS will then shift into PCs or Macs as well, so we do have a standalone mobile version that comes with that introduction, and then we move those customers into our core subscription service.

The third is we are still going after the standalone revenue from mobile. It's not huge. We have a free product, but we also have a premium product that we allow customers to upgrade to, so it becomes a relatively small but faster growing part of our revenue story.

Then lastly, as we—our net—we've had about 35 million different downloads of Norton mobile security that runs on all these different consumer devices. That develops a lot of telemetry that we can then go ahead and build into that unified security database that Amit's going to talk about later that help powers the telemetry and powers the intelligence behind some of our enterprise security products and services. So mobile continues to be very important as an integrated part of Norton Security and Symantec, though we don't expect it to become as large of a revenue source as we currently get off the PC security market today.

So let's talk a little bit about the state of the Norton business. As we mentioned, we did a lot of work last year to improve those margins up to about 53%. A lot of that improvement did come from exiting some of the unprofitable OEM deals that we had, but we executed in a lot of other areas to improve those margins as well. We exited out of brick and mortar retail in some countries where brick and mortar retail was becoming less interesting and certainly less profitable. We took a lot of our marketing dollars out of that brick and mortar channel and moved it into digital, and then we ended, like, several smaller products that had been kind of experiments over the years that weren't generating that kind of revenue. So it was kind of a broad look at the business and a broad look at streamlining, and a lot of that streamlining happened in the latter half of the year so we'll see some of the benefits of that from a cost structure into FY16 and '17, which gives us the confidence to say that we believe as we've achieved that 53% margins, we can stick with that same margin profile for the next several years.

We recognize we definitely have some revenue headwinds as well. We've talked about in the past we shift our—the policy around our auto renewal, which has temporarily caused our retention rates to drop, and we've also done some changes around the VAT tax in EMEA, which is a one-time impact that we have for—starting in January, but for most of FY16 of about 5% in our EMEA bookings. So—but despite those revenue headwinds, we're really able to continue to focus on increasing those margins; we'll be able to maintain those and generate that cash to be able to invest in the enterprise side of the business.

But I want to talk a little bit more about these revenue improvement initiatives. We really did three primary ones last year, and I'll go into each one of these a little bit deeper, but we shifted really to the subscription service and made it a much more simple product. We used to have a lot of point solutions. We're expanding our merchandising flexibility around sort of a good, better, best model which we believe will help both online and in-retail, expand our markets and focusing on improving the end-to-end customer experience. As these initiatives have started last September, we're starting to see the benefits of the improvement.

So as most of you know, the Norton billings have been declining for the last several years and what we can see now we believe we've sort of hit bottom and are starting to turn back up. So the December quarter we believe really was that inflection point and that turning point in our billings. We hit about a negative 8% in that quarter. But this quarter that just closed, the March quarter, we saw that improve to negative 6.5%, so we've turned that corner and we believe that that trend will continue to move upward from a billings perspective. It will take a little while until we see that improvement move in through to revenue, as our revenue is ratable over about 14 months, as well as some of the changes that we make in our retention we see the benefits of in 12 months and then the revenue flows from there. But we have turned that corner and are moving upward.

We've currently set ourselves a target in FY17 of revenue decline between negative 3 and negative 6% and started focusing on that midpoint of negative 4.5%. Thomas is going to go into that a little bit deeper. But we believe given the changes, we'll continue to improve beyond that over the next several years as we move this business back to getting to that market growth rate of about 2%.

So I'll go ahead and dig into some of these initiatives a little bit, and some of you may know that, for many years, Norton kept releasing a new variation of the product each year and we got to the point where you had about 10 or 11 versions of Norton and it became very confusing to our customers. Do I buy Norton for my Mac, Norton PC, multi-device, Norton

mobile, Norton backup? So we simplified that starting last September into a single subscription service that covers all your operating systems and all your devices. It's really simplified that purchase experience for our customers, and that's part of why we see this improvement.

We also shifted from this kind of annual product buy to a subscription service. Much like Netflix or your gym membership or your cable, you sign up for the service and you're in for that service to stay protected. As you change devices, move devices, your subscription stays with you, and that's given us the big advantage of getting a lot of our customers back into the auto renewal, and as always, we continue to enhance our security in all of our different releases. So that was a big shift for us last year, moving from that very complex portfolio down to that single subscription service.

Now, just this past March, we have increased a little bit of our flexibility around merchandising, released sort of a standard, deluxe, premium, good, better, best; that's really differentiated by the numbers of devices that you might want to protect. We've also increased some of the features around the premium product by adding our Norton protections, family protections, parental controls into that offering.

Finally, customer experience, and as we look the Norton business, we don't look at—we look at that there are many small things that we think we can do to go ahead and mitigate that revenue decline. When you've got 63 million customers, you can make relatively small changes and end up seeing a big impact. So as we focus on customer experience, both fixing some of our short-term things around making it easier to subscribe, easier to renew, easier to download, for every one point we see in our retention rate, that can generate over $10 million in billings initially and over 25 million over the lifetime of those customers that we stay into the business. So these little changes in customer experience can add a big impact to our business.

Over the long term, we continue to work on improving the end-to-end customer experience, and as we start to see the consumerization of IT and BYOD, we know that a lot of our customers are going to take their personal devices into the enterprise and we also want to make that a very seamless transition. So we're working to ensure that both the Norton and the enterprise security really can take advantage of the coverage that we have in the Norton marketplace. So I've got a couple of examples over there. I'm not going to really hit them due to time, but just to note that these things around our ecommerce platform have big effects for our business.

So what's coming up? A couple of things I would hit on the product roadmap for 2016. The first is sort of on that bottom row. This new simplified subscription service was rolled out in many markets last year but we're going to continue propagating that through all of our channels and all of our markets. We rely on service providers like Comcast, Deutsche Telekom in Europe, SoftBank in Japan. They've been still working on the legacy product set, so this quarter, we'll be moving to them to the new simplified service and we'll start seeing the benefit through that channel that we're seeing in our direct channel. We'll also be starting this year to migrate our customers who are on the legacy portfolio of SAV (phon), Norton 360 to the new Norton subscription service this year as well and complete the propagation to Japan through APJ this year.

The other big activity that's happening in the consumer world this year, as you all are I'm sure aware, is the upgrade to Windows 10, and that's a very important change for our customers. So we've worked closely with Microsoft over the past couple of months to ensure that that will be a very seamless transition for our Norton customers. They'll be able to continue to have a very smooth transition as they move to Windows 10 with their Norton Security product, and we actually believe that will be an important inflection point, moment of truth for our customers where we'll look to reach out and make sure they're aware that Norton will work very effectively on their Windows 10. So a lot of other things coming out on our product roadmap that we think will incrementally improve the business and that revenue performance.

On the go-to-market side, I mentioned a little bit, a big shift away from the brick and mortar retail to reaching out to our customers directly online. As part of that, we really invigorated a lot of our messaging around what's different. Norton is a premium product. There are a lot of competitors in the market, but we have clear differentiation around the level of security and the quality of protection, the way that we provide customer support 24x7 in most languages around the world. These are very differentiated offerings. We provide our customers a lot more information as threats break out to give them some guidance on how they stay safe, so we've refreshed a lot of that content to be able to make it clear why Norton is premium and why it's differentiated from the other products out there in the market.

As we also expand into other markets, local payments become really key. When the online channel is really important to you, that becomes really important. We launched local payments in Brazil and Mexico last year and saw a double in the amount of online business that we were doing in those markets, so we'll be expanding more local billing, more local payment methods in a lot of markets around the world this year.

We're also looking for new digital partnerships. I mentioned some of the longtime Norton customers, but we actually signed a new, a telco in Brazil, America Movil last December, and they've got over 300 million subscribers and they'll be launching Norton into their base starting this quarter. So we expect to see some expansion in Latin America to help with the revenue generation for the business, so a lot of focus on improving the go-to-market, primarily focusing on those digital channels.

So just to kind of sum it up, I think that we will—the Norton business I think is in a growing market, albeit slowly growing, and we'll benefit from that slow growth of that PC security market. The threat landscape continues to be very challenging for our customers, so they'll be searching for the best level of protection in that market. We think last year's success with reducing the complexity of the business and improving those margins is something we're going to be able to stay with for the next several years, and the organization will be continually focused on improving our revenue performance. As I mentioned, we're very happy that, from a billings perspective, we really turned that corner in the December quarter and are moving upwards from there. So we have our target (inaudible) by '17, but we really don't see any reason why, over the next several years after that, we can't get the Norton business back up to the market growth rate.

So I'll hit you with one more point before we take Q&A. The Norton business has evolved over the years. For many years, it was really just about the PC and now, as I mentioned, everything is around multi-device, about protecting the user, protecting the household, protecting the information across PCs, Macs, tablets, mobile devices. But we're also very aware of consumer IoT and IoT in general as a company. We believe that eventually, households will be filled with the internet connected devices; we'll move from where we are today at six or seven per household to dozens or over a hundred per household, and that opens up a wide threat vector for the bad guys to attack our Norton customers. So we've been evaluating the different technologies, and we've got some beta product that we've already built that can provide a certain umbrella protection over what will be a very heterogeneous internet connected home. We're continuing to make those investments, both on the consumer side, as well as we partner with the enterprise side of the security business as folks see more of an embedded security strategy. So while won't be releasing any products here in the short term, we've got our R&D going, we've got a beta completed and we'll look to expand that as we take sort of the pulse of that market.

So that's the presentation. I've got about 10 minutes or so for questions, so I think, Helyn, if you want to come up and facilitate that.

Helyn Corcos: (Inaudible). Brad's got a question.

Brad Zelnick: Thanks. Brad Zelnick with Jefferies. Fran, that's a very helpful presentation. You didn't give us explicit top line guidance for '16, but from everything you've told us, it would seem that that business—the business would have to be down double digits, and at the same time, you did tell us that you should be able to maintain low 50% op (phon)

margin, which would imply that there's a tremendous amount of cost that can still be taken out. Can you maybe just frame for us where that comes from, and specifically, if you could talk about what is left, in terms of OEM placement fees, how much of that will be funded from those placement fees and then what does that look like in years to come?

Fran Rosch: So Thomas is going to give you some very explicit guidance for '16, but I will tell you the business is not down double digits, so if that math came out somehow, that's not right, but he'll give you that explicit guidance. So I think that we will maintain those margins. As I mentioned, some of the reductions that we did last year were in headcount and it took some time throughout the year to identify where that headcount was coming. So the headcount really was removed more in the Q3, the December quarter, and even some into the March quarter, so we didn't see the benefits of all that reduction last year when we were able to obtain those 53% margins, so even though our revenue's declining a little bit next year, we'll be able to match that from an expense stand cut (phon) as we see the benefit of those headcount reductions really flow into this year, in FY16. We also are finding better ways to do support, customer support, which is already a very competitive—less than 5% of our revenue we spend on support, but we're using more of an outsource providers to be able to make that more cost effective as well. So those are some of the areas that we think will go ahead and ensure that we can continue to deliver on those 53% margins in FY16.

From an OEM placement fees, really none of the savings next year come from OEM placement fees. We've already exited the ones that we were going to exit previously in FY14 and '15, so there's no additional. We're actually looking at possibly getting back into some OEM deals if they make sense from a financial standpoint. As we've improved moving our customers to a subscription service, that's improved the lifetime value of those customers, which means we can get more competitive as we go back in and bid on some of those OEM deals in the future. Now, that won't be any short-term benefit from us because the lifecycle of those OEM deals are about three years from the time that they re-bid, you win, you get back into the market, you start seeing the benefit, but we'll look at those going forward as they make sense for the business.

Steve Ashley: Hi, Steve Ashley, Robert Baird. I wanted to just get—talk about the regional (phon) marketing (cross talking).

Fran Rosch: Yes.

Steve Ashley: Market. Assuming there's been a learning curve…

Fran Rosch: Yes.

Steve Ashley: Assuming that you've got more efficient over time, maybe you can talk a little bit about that, and is there more efficiencies to have? Are there partnerships, are there things you learned, are there things you can do better just as you've learned how to better go to market?

Fran Rosch: Yes, absolutely. I think we have learned a lot but there is more to go. I think what we've learned is that there was so much—I think people think of digital marketing in paid search, and a lot of our effort was sort of going into paid search, so we really expanded our digital marketing well beyond that. We have a free trial program where we actually have about 12 million users every year that come in and free trial Norton. We believe there's an opportunity to increase the conversion rate of those from free to paid better than we have before, so we rolled out the new programs to really communicate to those customers better during that 30-day trial to get a higher conversion rate. That's one example.

Affiliates is another. We use affiliates to drive traffic to our cart and our store. We've added two more affiliates in just this past quarter. We'll see some benefits from those, Rakuten as well as oND, so we'll see that start to ramp up there. We also believe that as we improve our messaging, we'll become more effective in the ROI of our digital advertising spend, less about buy, buy, buy, renew, renew, renew and more on why and what's different about the Norton service

and the competition. So we think we've done a lot. I would say last year was a lot about optimizing the digital marketing in those individual channels, and I think FY16's going to be a lot about understanding the ROI of those—and comparing those channels against each other so that we can then shift our spend to get the maximum return for the business.

Aaron Schwartz: Hi, Aaron Schwartz. You talked about the move from getting the NAV in this space to the subscription service over the next 12-plus months.

Fran Rosch: Yes.

Aaron Schwartz: Is that the event where you—is that the event where you shift everyone from out to up, and what's your experience in the churn rate when that happens? Thanks.

Fran Rosch: Yes, so I think what we did is when we launched the new subscription service back in September, we launched it for acquisition only, so all the new customers came into that flowed through the subscription service through Norton Security, so it was a good opportunity for us to learn without necessarily going and putting any of that large customer base at risk. So we feel like we've learned a lot, we've made the tweaks that we needed to do around the customer experience, so now we're ready to go after that install base and shift them over. We've worked very hard from a product standpoint and a customer experience standpoint to ensure that that's like a one-click shift, so in the past with Norton, you'd have to actually uninstall your old product and then reinstall the new one. That is no longer required. It's a one-click, everything happens behind the scenes so the user stays with that, so we feel pretty good about that.

When we see the—in the old days of the AR opt-in models and then we went for AR transparency, as we move people to sort of subscription services, we're seeing very similar opt-in rates to AR as we had when we had the old AR model. So I think we're going to sort of get back to similar AR rates with the subscription model that we had in the original model, which bodes very well for the business because that will really strengthen our core subscription base.

Fatima Boolani: Hi Fran. Fatima Boolani from UBS, right here.

Fran Rosch: Great, sorry.

Fatima Boolani: You had sized the mobile market at about $200 million growing at 15%, so it's growing very quickly so maybe a two-part question for you. Why is that market opportunity still very small from a nominal perspective, and perhaps, have you considered partnering with some of the larger carriers vis-à-vis this product opportunity?

Fran Rosch: Yes, I think the reason that the mobile market is just smaller is that consumers—there is two main reasons. Consumers just grew up with the paradigm of free applications and expecting everything free on their phone, so that's kind of—they're comfortable with that. There are also some very small companies that got started out and thought they would make their name in mobile with a free service, so that's just kind of a paradigm that's accepted by the consumers at this standpoint. Also, if we look at iOS and to somewhat Android not quite as much, those operating systems are more secure. There's less issues now. They're growing, especially on Android, so we'll see how that market develops over time, which is important to why we want to be there, but I think those are the prime reasons that it's smaller. It's just the—they're comfortable with freeware and the lack of the real security issues.

Where we do see the potential though, as I mentioned, in those applications, so as consumers, especially in Android there, become more and more different app stores that are less curated, as well as, say, Google does with Android store, there could be a problem with those applications. So we're seeing more and more in a rise of malicious applications, which is something that we're watching very carefully. So I think that answer—was there a…?

Male Speaker: I wonder if I could add to that. One thing that we are seeing is that our enterprise customers are becoming increasingly concerned about mobile users because it's easy to introduce a threat into the enterprise from mobile devices, so there is some interest from enterprise customers understanding how can they support—how can they have a more secure environment that might include securing mobile endpoints, even of the customers of theirs using mobile devices or supply chain, et cetera. So as that becomes a more important trend, that's a really important synergy then of the consumer business and the enterprise business because we'd be able to provide better protection in kind of an environment where the perimeter is very fuzzy and/or maybe doesn't even exist anymore, by ensuring that more customers of enterprise companies are protected with Norton. So we'll have to see how that develops.

Fran Rosch: That's a good point, and we've actually done a lot of work to actually integrate the consumer elements into our enterprise information protection strategy that Balaji will talk about next.

Helyn Corcos: We have time for one more question.

Gregg Moskowitz: Hi Fran. It's Gregg Moskowitz from Cowen. I just would like to go back to the expected revenue decline you sort of laid out for fiscal '17, the minus 4.5% at the midpoint, and if you look at the market, it's been fairly well documented in terms of what we're seeing in the landscape with regard to free and premium type offerings, so would just love to hear more about, if you could elaborate on your confidence level why you think you will get back to growth or to a level that kind of is at or roughly near the market growth rate of 2 or 3% in fiscal '18 and beyond.

Fran Rosch: Yes, I think our confidence is really high that we'll be able to do that. Some of that is because we're seeing the impact of the changes that we made in the past year and the fact that we sort of turned that corner and are moving upward. Norton has a very large and loyal install base and they're very effective—we're very effective at retaining those. I also think that threat landscape continues to get more complicated and freeware just simply is not able to protect customers from those threats. We acquire—a lot of our customers have been living in freeware for several years and found that they weren't able to stay protected. So as we continue to ensure that we're in the best security, we think that will drive more customers to us as we go through.

I also think the customer experience—and again, it sound—maybe it sounds like small ball, but these are changes that as we make, really grow that install base quite a bit. So we think we feel confident that we'll be able grow with those market rates in the future, but right now, we're focused on delivering for that negative 4.5% in FY17 and then we'll focus on moving toward that market growth in the years after that.

So thank you very much. We're going to go ahead and segue from the consumer business now to the enterprise side, and we have three presenters who are going to present, Jeff, Balaji and Amit, and it's my pleasure to introduce Jeff Scheel as your next presenter.

Jeff Scheel: Thanks a lot. Good morning everyone. As Mike mentioned, I'm one of the relatively new executives with the Company, so I am now officially in my seventh month. I'm not new to the security market, so this is my 11th year in security. Some of you I probably spoke to in the fall of 2009 when ArcSight did its Investor Day at the NASDAQ Exchange, and so I had a very similar role at ArcSight through the merger with HP. More recently, I had a similar role for Mandiant and worked through the integration with FireEye, and I most recently came from FireEye. So my background is really most recently, last six years in network security, incident response and high end managed services, so what I've seen is some interesting developments in the last 11 years.

So what I'm going to give you is some context on the threat landscape and specifically what I want to do is share some of the statistics from our internet security threat report that Mike mentioned, which you can all download a copy of. Then talk to you about some of the unique capabilities we have and personally want—you know, some of the reasons why I'm so excited to be here, and then finally, I want to translate those into the growth drivers for the business and give you an indication of why we think the strategy that we have can be successful and show you how we're going to be able to

access expanded markets. Then I'll hand over to Balaji and Amit and they will take you in much more detail through the product strategy, actually talk to you about our unified security analytics platform and help you get a much better understanding of how these apply to the threats that customers are seeing.

So the first thing I would say is when I got into enterprise security, it was really at a time when identity theft was very nascent. It was a cottage industry. It was sort of small-time crooks stealing people's credentials. Now, as you know, this is big business, okay, and one of the things that attackers exploit is the fact that, as an IT industry, we're constantly innovating and we do that to drive the business forward, but we rarely do that today with security in mind. So if you look at everything from the broad IoT market, including industrial control markets or IoT for consumer healthcare, all that innovation moves ahead without any regard to how you secure the data, right? So there's always a gap for our customers that they have a challenge closing, and that's the first thing that's just endemic to the IT industry, right? So until the IT industry really takes security serious at the time that they create things, that gap will persist.

The second thing that, frankly, is—makes the—well, first of all, it makes the industry very, very interesting because this is not like delivering ERP software. The fact that every time we deliver something into a market, there's somebody on the other side who's trying to defeat it, makes it a very, very dynamic market, right? So if you look at some of these statistics from our IFTR, five out of six large companies are now targeted. That's a 40% increase over last year.

Malware is getting much smarter so what does that mean? Well, certain types of malware now know if they're being asked to run in a virtual environment, so that means you have to use much more advanced techniques to detect that malware. The variability and the customization of malware that Fran talked about, it's even more prevalent in the enterprise space than it is in the consumer space, and so we've reached kind of a new plateau in terms of the level of innovation on the other side, so in the most report, we highlight that we have an all-time high of new zero days, okay, so 24 zero days. Last year, it was 23, but in the prior 10 years, the number hovered between seven and 12, so in two subsequent years, we're seeing that the zero days stay at a constant level and it's reflected in the increase in attacks across the different verticals, right? So there's headlines between every one of the industries that's listed there.

The other thing that's going on – I think some of you have written about this – is there's a research in the traditional endpoint at the same time that there's this move to mobility and IoT. Why is that? Well, the endpoint is the only place where the data may be unencrypted, right? So as we've encrypted more data when we move it around, the place that you get at it is when it's unencrypted on the endpoint, so it really makes our SEP solution in large customers much more relevant as a market we can go after with some of the advanced solutions that you'll hear about from Balaji.

Despite the fact that some of the darlings of our industry are benefiting from essentially next generation firewall or in-network capabilities, the reality is a big part of the workload is moving out of the traditional network, right? So what you have to have are solutions that contemplate the fact that 30, 40, 50% of the work is being done with users connecting directly to cloud resources where they never come through a VPN, right, so you don't have the same level of control. The capacity on a mobile phone is enormous. I can go—as a Symantec employee, I can tell a salesperson, "Send me a briefing," and they can send me a 12 megabyte PowerPoint, I can bring it up on my phone, right? That's a fairly recent phenomenon but it means that you have to assume, in many cases, that your data is in the wild and that's the reason our information protection strategy is going to be so important to customers going forward.

The other thing that's going on is there's a rise in demand for services, okay, and in my time at Mandiant, I saw this because we would go in, we'd respond to a breach, right? So it's like basically the firemen showing up to put out the fire, right, and then as the IR team would pull out, the customer would ask, "Well, how am I going to prevent this in the future? I don't have any of these skills," right, and so that's an enormous opportunity for our managed service capabilities and for some of the advanced services that you'll hear more about.

Then finally, cyber security really is a national issue. It's a nation state issue, and so you see all the attacks that you've seen recently that have a nation state component to them mean that governments are dealing with this issue and,

frankly, we've had a lot of conversations with government officials. We had our government symposium this week and Mike and I met with a lot of lawmakers and policymakers who are struggling with how we deal with this at scale. So it makes for a very dynamic environment.

So what assets do we bring to the party here? Well, the key one is our presence on the endpoint, because despite what my old boss said or what other competitors say about putting agents on the endpoint, it's not nearly as easy to do that, and if you go—any of you with a major money center bank, if you go talk to your CIO about how long it takes to validate and endpoint client or endpoint agent, it's about two years because, for productivity reasons, you can essentially do no harm, right? So that presence that we have globally is huge and our ability to deliver solutions into that franchise and into these other franchises like data protection and email security is a huge opportunity for the Company.

Behind that, as Mike mentioned, is all the telemetry that we gather, okay? So it cuts across these hundreds of thousands of endpoints, the attack sensors we have out in the wild and across our email gateways. Now, what I like to say is it's not how much telemetry you have; it's what you do with it, and I think what you're going to see in a minute is we're doing some very, very interesting things and we're delivering some capabilities that people cannot get from any other vendor based on this information.

So how does that translate into market opportunity? Well, you've got a core market that Mike—as Mike mentioned, is growing at 10% but with some of the things that we're going to do, we're going to be expanding our total addressable market across some key segments. So if you look at threat protection, that's a relatively new market for us, what you're going to hear from Balaji is the way we deliver into that market is very, very unique. It's different than point appliance players. Why? It's because we have that presence across endpoint email. We also have the largest intelligence network in the civilian world, and so we're going to instrument that network and make that intelligence available back into our customers. We're going to put a window on that intelligence in a way that's never been done before.

If you look at information protection, there's a whole set of issues now with the perimeter going away that involve creating a new perimeter that sits at the intersection of identity and context that you have about location and so forth. That becomes a huge opportunity for us on prem, but more importantly, as people move to the cloud we can deliver that into the cloud. Then finally, the services market is exploding and the reason is this stuff is just—it's very hard to do. There are not enough experts to be able to hire and retain them. I saw this in my time at ArcSight. Our SIM deployments were never as solid as the day we turn them—over time, they were never as solid as the day they were turned on, and the reason was it's hard to maintain, hard to retain the personnel, and so we see that as a huge growth opportunity.

The final thing I would tell you is this—what's exciting about this business is it's a very, very mission focus business. The people that work on these problems take it very, very seriously and we've got to do the same thing as a vendor, and I think with the team that you'll see today and with the commitment we're making to some of these solutions, we've got some very exciting times ahead.

So with that, I'll hand it over to Balaji.

Balaji Yelamanchili: Good morning everyone. I know it is late morning. Thank you, Jeff. So I'm going to build on what Jeff walked us through, and that's the market opportunity around the Symantec enterprise security and I'm going to cover product strategy, together with Amit Mital. We're going to go a little deeper on this in terms of various areas that Jeff alluded to; also going to touch on the roadmap briefly and a little bit around the go-to-market before we actually spend a little bit of time talking about the questions and answers.

So at the highest level, Mike alluded to today our mission actually continues to be protecting the businesses, whether they are actually the businesses of the government organizations, keeping them safe from the ever-evolving digital threats. That's how our high—at the highest level, it's our mission. Our strategy to accomplish this mission focuses on

four key pillars. So first and foremost is threat protection and when we talk about the threat protection, we're talking about protecting the infrastructure, the entire infrastructure from these threats. It's endpoints, it's the data center, it's the gateways, it's the network; it's all the control points that you actually—the attackers normally try and breach.

Within the context of this, obviously there has been ever-evolving threat landscape where the traditional approach to the strategy is now evolving rapidly into highly sophisticated attacks, where the attacks are very polymorphic, and what we mean by that is they're very one-off, it's not something that has been seen before and they come in very fast and they come in and hide there for a long period of time in the context of the advanced persistent threats, and then they try to kind of find the vulnerabilities in your system and then try to ex-filtrate the information from that point on. So it is extremely important that the threat protection really is not just covering the prevention aspect but also the detection and the response and to do so across all the control points in an infrastructure in the data center that you're talking about.

But as Jeff alluded to, the information that the attackers are really trying to go after is not necessarily always inside the four—inside the firewalls. It's actually moving more and more into the cloud and more and more into the mobile devices that are actually operating on unprotected networks and so the ultimate prize is really the information. The prize is not actually breaching an infrastructure; the prize is breach the infrastructure and actually steal the information, and so you have to really kind of think of this information protection not just in the context of protecting the infrastructure but actually protecting the information as it moves to the cloud and the mobile world.

Regardless, as a result, the data, wherever it resides, it resides on-premise, on the device or on the—in the cloud, you really want to be able to protect that. We want to be able to really anchor these two things with the critical important piece of the puzzle, and that's our security analytics platform, and the reason it is very important is because you really want to be able to really get the context and the correlation across various control points, across these data sets that are moving from inside the firewall to the outside the firewall, into the cloud and back and forth. The data is at rest and the data is always in motion, and you really want to be able to really try and understand what the telemetry is and how you mine this data, how you actually analyze this, how you get additional insights and then how do you actually proactively protect yourself. So the analytics actually become an important piece of the puzzle here.

Then finally, customers are asking for a lot of this as security as a service. The box fatigue is extremely critical issue right now. But when they're asking about this, they are not just asking about, "Just come in and monitor my service or my infrastructure that's out there, the security infrastructure. I really want to be able to really provide the full end-to-end set of services, monitoring, incident response, simulation, ability to really kind of proactively address a lot of these things so that I can be better prepared through the modeling and other kinds of aspects." So this strategy, the Symantec enterprise security strategy, is very broad and deep, it's very ambitious but we believe it is highly achievable. The reason is because it is built on some enduring differentiators that we have.

We have a very strong presence across many critical control points, endpoint, the gateways, the data center, etc. Second, we have an unrivaled amount of telemetry that we can actually use to better actually predict the outcomes if we can actually mine and analyze this information effectively. We have a great set of security technologies and the engines that are well beyond the traditional antivirus signature approaches. Behavioral analytics, predictive analytics, wisdom of the crowd, a lot of different techniques that we use in order to be able to actually detect and protect a lot of these things. So these strengths actually do allow us to be able to really achieve the kind of division and the kind of the strategy that we're actually talking about. That combined with the focus that Mike talked about this morning and the passion and the commitment that Jeff talked about among the team and the incredible mission that actually we're all really working towards gives me a very, very highly optimistic view of why we think we can win in this market and get our fair share.

So what I want to do is to double click on each one of these things a bit. First and foremost, when it comes to the threat protection, I alluded to this, while historically most of the posture from the security vendors as well as the companies

have been on the top right hand corner quadrant and that's the prevention posture, we do know that the compromises do happen, particularly because the attacks are much more sophisticated and so it's equally important to be able to detect and remediate as soon as things actually happen. But what is important though is how do you really do this not just within the context of a single control point like network or endpoint or in a gateway or in the context of the data center but to do so across all of them.

That brings us to the strategy, and that is that Symantec's threat protection strategy centers around four key areas. The first area is this Advanced Threat Protection across the control points. I'll talk about why this is actually very important in the next set of slides. But once you actually detect these advanced threats it's equally important you conduct the necessary forensics extremely fast and then you effectively remediate a lot of these things in the fastest possible time. So, detection is not adequate. Prevention—the forensics and the remediation is equally important. But the thing that I mentioned to you earlier is more and more of the workloads are actually moving to the cloud, and so it's not simple, it's not enough rather to actually try and protect a lot of these things that's actually inside the data center or inside the firewalls.

You really also want to be able to really protect the workloads that are actually moving to the cloud if something actually moves to the Amazon, for example, where you're actually running an important workload into Amazon. Amazon actually does not really care what exact, specific workload you're running there and who is coming in and accessing that. It's the responsibility of the organization that's actually running the workload. They will protect their core infrastructure and they will guarantee that for you, but what's actually happening inside the workload, who is actually coming in, what data they're actually creating, consuming, extracting, all that is actually the responsibility of you, the customer, that's actually running these things. So, when we talk about the threat protection it's not adequate to kind of think of this as the network and the endpoints and the gateways that are actually in the traditional realm of the data center but also as things move to the cloud as well.

Then finally, managing all of this using the cloud-based infrastructure. There's tremendous economies of scale with the cloud, as you all know. It actually helps the customers obviously focus on the security versus actually having to manage and install and deploy and configure all these things on an ongoing basis. So what is important is really how can we bring more of the cloud computing capabilities from a management perspective so that the customers can focus on the traditional tech security posture as opposed to having to worry about the IT and the systems integration?

So what I would like to do is over the next two, three slides just walk you through very quickly what are the fundamental capabilities that we're talking about and how they're differentiated compared to anything that's out there.

First and foremost, the Advanced Threat Protection. What we're talking about here is certainly detecting these very sophisticated APTs, the zero-day attacks, and all the related things that the attackers are really going after. But as I said, it's really across a very specific set of control points that we have very good visibility around; endpoints where we have a strong presence, email where we have a strong presence, network where we partner very effectively with many of the firewall vendors today.

What we'd really do with that is a very effective cross-correlation and instant prioritization. Why is that important? When actually a file comes through the network and if it is a traditional next-generation firewall, they will actually look at that file, they will want to know what that file is and they will want to know if it is good file, let it go, bad file, stop it, if it is unknown, suspicious, take it and then try to see if you can detonate it and then execute it and see if you can actually provide a verdict.

We do the same thing. But we go a step beyond. We also like—take a look at that and see if that's actually also been found in the endpoint, that's also been found in the email. Why is it important? What is important is if I found something in the network sensor but then I also found it in the endpoint and then I found the endpoint already blocked

it because of Symantec Enterprise Protection, the endpoint protection, then I know that I can actually put a lesser priority on that and then focus on the ones where I'm actually finding this issue across all my control points.

So this issue of efficacy and the least amount of false positives is a very, very important issue when it comes to this advanced threat protection. The analysts are highly fatigued. The reason is because there are too many alerts and too many false positives and they want to be able to really minimize these things and focus on the things that they have to focus on and this cross-correlation across the control points is a very, very important aspect of it.

Obviously going beyond that, how do you really detect these advanced threats? There is this idea of the sandboxing and the payload detection or payload detonation. So these are the techniques that are very effectively used by the vendors to actually thwart these attackers. We do the same thing. But we go a step beyond that. What we do is actually we do this payload detonation in the cloud exclusively. Why is that so? Because as the volume and the variety of these things go up you have to have a massive computing capability to be able to really real-time detect a lot of these things and to do so on a set of appliances that you have to constantly upgrade is actually not a very, very scalable model. But the more important reason is because when you actually try and do that in the appliances with the limited computing what you try to do is actually you try to do it in a virtualized mode.

As Jeff said in the latest ISTR report, 28% of all malware is now actually virtual machine aware. What does that really mean? They actually know that if it is actually inside a virtual machine they actually will stop actually doing what they're supposed to be doing so that they can actually hide from that. In the cloud you can actually do any type of execution (inaudible) in a very cost-effective manner. Try and do that using an appliance on the on-premise is extremely difficult and not at all cost-effective.

So this cloud-based approach to this payload detonation becomes a very, very important element of how you actually stay one step ahead of it. But as I said, just detecting is not actually adequate. You really have to go a step beyond that. Now you've got to really now say "Once I detect it I need to understand where all this particular thing has actually creeped in. How do I do the—conduct the quick forensics and not just with this group of people but actually a set of tools that can automate a lot of this forensics capability? I want to be able to do that in a closed-loop fashion." What really I mean by that is I want to be able to do that by sitting inside my advanced threat protection solution as opposed to having to go to yet another tool. One of the reasons we actually have this advantage is, because we have a tremendous presence in the endpoints and the gateways, we actually can orchestrate and control and then remediate a lot of these things from within the same console as actually having to move it to some other agent. If you take just the network only, that ATP solution they will be able to detect it but in order to be able to do any of the remediation now they have to move all that context to something else, or maybe create yet another agent to run on the endpoint and then Jeff talked about why that is actually not easy.

So the differentiator for us here is it is about the efficacy and it is about the least amount of false positives but to do so in a cost-effective manner. That we believe is ultimately going to help quite a bit in terms of the customer staying ahead of it and which also gives us a kind of a critical differentiator that we need in the context of the Advanced Threat Protection.

So complementing that as I said is the remediation and in order to do the remediation we talked about this forensics aspect of it, and so one of the key things we try to do is we have two choices. We can actually do a lot of this forensics remediation using yet another agent or actually take the existing agent we have a lot of presence in and extend that agent with these extensions critical to this remediation and forensics including very fine-grade policies that you can actually apply to do this remediation and to do that with a very, very fast set of forensics using the flight recorder concept that actually the airlines and others use pretty effectively as well, and then do so across multiple endpoints as opposed to a single endpoint at the time that typically an IR team tends to do when it is actually manually run.

So again, the differentiators here for us are that how can I actually bring this type of capability in an integrated manner with the ATP but to do so with—you know, without new agents, with an easy upgrade, with an ability to do that in a cost-effective manner? That we believe is actually going to be a very important value proposition to a lot of our existing customers as well as to the new customers.

But then I said the puzzle is not complete if you're just thinking about it in the context of what is inside the firewall. You have to also start thinking about it in the context of the workloads that are moving to the cloud and apply some of the same capabilities; things like file integrity monitoring, things like application hardening, things like control and the compliance. These are the things that above and beyond what you actually do on a typical endpoint with the antivirus, the malware protection, detonation and signatures. All the things that you do on a typical endpoint you have to do that on a server workload as well but you've got to do much more than that because the real applications and the real data is actually sitting there and so really you have to control that in a much more fine-grade manner than what you can do here. So that's really what we're talking about and to do this from a strategy perspective and from a product road map perspective we're taking our existing data center security capabilities and extending it to the cloud workloads including the support for virtualized environments like the VMware, NSX, ESX, but also the Amazon and the Azure and any open stack-based cloud including the rack space.

So the summary here is from the standpoint of where we are we believe that these are very important elements of the overall threat protection, the advanced threat detection, the forensics and the remediation, the server workload protection, do it all using a common management but running from the cloud. From a delivery standpoint we are really looking at delivering the ATP actually this fiscal year, starting actually—literally starting this current quarter and then progressively add more features to that and then the same thing on the forensics and the remediation as well and then at this time the server protection as well we will be adding this through the course of the fiscal year for us.

As a result of it we think that there is actually a key revenue opportunities for us that manifests into some of the incremental revenue opportunities above and beyond the traditional TAM that we are actually operating. This is the expanded TAM that Jeff actually talked about being able to go into install base into our existing endpoint customers, existing email customers and to be able offer these as add-ons is actually a very, very effective way to really increase and tap into the expanded TAM that Jeff talked about. But it is not limited to just the existing install base. We believe that we have a very, very strong value proposition even to those customers, the net new customers because of the kinds of ways we are really solving these ATP problems as well as how we're actually automating many of the typical IR project activities. Then what we're doing in the cloud is actually applicable to either an existing customer or the net new customer.

So next up is the information protection. As Mike said this morning, whereas threat protection is about, you know, keeping the bad guys out, the information protection is about keeping the good stuff in, and—but as you know when it comes to the information while historically the information was created and concealed inside a firewall particularly in the context of the enterprise more and more many of these applications and the data that actually these applications are creating is moving to the cloud, as well as the users that are actually creating and consuming this information is also moving outside of the traditional parameter onto the mobile devices that may be running on networks that may or may not be reliable 100%. In fact, many times an employee of a company that is actually using a mobile device that is actually then using the service that you subscribed for the employee to use a Saleforce.com, to use a Workday is probably actually never coming through your network. They're actually literally going from their device operating on a network directly into a Workday or a Salesforce and doing whatever they can, but they're doing so with your information. They're creating and consuming information that is important to you using the identities that you actually provided them. So the holy grail is really about protecting that, protecting the information and protecting the identities as opposed to just protecting the threat landscape that we're talking about threat in infrastructure, threat protection in the context of just infrastructure. So we think that it is extremely imperative when it comes to information protection that it manages the information regardless of where the information is. It could be on-premise, it could be on the device or it could be in the cloud.

So our strategy really centers on a couple of very unique things. We have some really strong presence in the data protection and the information protection over the years. Our DLP, the Data Loss Prevention, is actually one of the highest market share products that we have in our portfolio. We have a very, very strong encryption technology. We have very strong authentication, an access management set of technologies. We have two-factor authentication that we actually add on top of that for strong op. What we're really talking about is extending our existing assets but in a unique manner to really address this phenomenon of the cloud and the mobile and do so not just in the context of the information protection from a DLP and identity management but also layer the analytics that are very critical so that you can actually see the user and the behavioral analytics. In fact this term that you hear, UBA, the user and behavioral analytics, is now becoming one of the most important elements of the overall security market right now.

So what exactly are we doing here from a product perspective? What we're doing is we're taking our existing DLP technology and our existing identity and access management technology and we are now combining it in a very unique way with this analytics, the user behavior analytics, and creating this new cloud control point. We call it CSB, or the Cloud Security Broker. You might have heard the term CASB, the Cloud Access Security Broker. That is a subset of what typically a CSB does that's primarily focused on the access. Here we're talking about the access control but also a data protection that you bring along with it. What this really does is if you are actually a mobile user, if your customer for example is a mobile user and they actually have the access to something like a Salesforce or a Workday, as they try to go from the mobile running on a network to the cloud there is actually a broker that we actually put in between so that it actually for a test to come through this CSB that we're talking about. By coming through this you now have a full visibility into who this user is, what kind of authentication and access privileges that they have and in context also apply to the data prevention policies right then and there. You do that with a high contextualization. You actually know who the user is but also what device they're using, what location they're in, what kind of policies that you have to apply. Is somebody's actually accessing something from, you know, the United States near the—you know, where they actually normally live or where they work? Perhaps a traditional authentication might be okay, but if they are trying to do this at odd hours, you know, somewhere in Belarus on a network that you actually don't have much information on, you may want to actually challenge them for a much stronger authentication. You may want to actually prevent them from downloading anything even if you think that they're actually a legitimate employee. To be able to do that in context right from within there is extremely important and then something like a Cloud Security Broker is a fundamental way to actually do this.

But then as I said, complementing that with the analytics really now helps you from that idea that information protection is about keeping the good stuff in and so now you can actually do all kinds of behavioral analytics because you have access to all this telemetry and the profile the users and the activities and the data flow and thereby you can actually see if there are certain anomalies that you actually find and if so how do you really detect this fast and then prevent this very fast. So, this idea when it comes to the information protection is this whole notion of taking the existing prevention and the access management capabilities we have on on-premise and extending it to the cloud and the mobile and then layering this with the user behavioral analytics becomes actually a very, very important puzzle to the more of a 360 degree view of the information protection that we're talking about.

As I said, this is not actually something we're building from scratch. We have actually existing assets. We're continuing to actually add more and more cloud capabilities to our DLP, to our identity and access management, to our analytics capabilities and then over a period of time through the course of the fiscal year '16 you will actually see us deliver the full suite including the Cloud Security Broker as well as this whole UBA concept that I talked about.

We believe as a result of these things that the monetizability of these things is actually very, very solid. Again, both in the install base where we have strong presence, where we have a lot of customers moving to the cloud and the mobile so they can take what they do with us on the on-premise and then extend it using the additional add-on modules but also we believe that it is actually tremendously useful for a lot of the net new customers that are moving to the cloud.

So, the third area that I talked about earlier was this how do you really provide these things from a security as a service perspective? The reason this is very important as Jeff alluded to is more and more people are saying, "These are all great things but these are sufficiently sophisticated and can you actually help me? I am not the largest bank in the world. I'm not the largest manufacturer in the world and I really need more expertise and I have a skill shortage and I want to be able to do these things with your help. Do you provide security as a service?" It's a managed security in terms of operating a lot of these things, but also there is a traditional monitoring service that we have been actually very strong in for many, many years.

If you look at our monitoring service, which we have been providing, it's a collection of technology as well as the people. The technology to actually collect a lot of this information and analyze it and disseminate from a monitoring standpoint for 24x7 but we also have physical security operation centers around the world that we actually staff with very, very experienced security analysts that in turn actually monitor and maintain the security postures for many of our companies, many of our customers, rather. But as you heard Jeff talk about, as you heard Mike talk about, what is important is more and more customers are saying, "Monitoring is not adequate for me. I also want from the same vendor an ability to really react and respond if there is actually a compromise but in conjunction with the monitoring infrastructure that I already have as opposed to going somewhere else. More importantly I want to do a better job of preparing for a lot of these things proactively thereby if you have all this global intelligence how can I tap into that and then how can I correlate to what I have so that I get actually a better experience than just actually doing it all in silo."

So this idea of threat intelligence, service, the monitoring service, the incident response service, layered with this whole simulation capabilities is actually a combination of the services many of the customers are saying from a security as a service that when they put it together properly, if they're integrated properly it actually will help me a lot better in terms of preparing for something proactively, reactively or even during the attack.

So when it comes to the portfolio that we have within the server security services we have a very, very strong presence with our monitoring capability. In fact we've been in the Gartner Magic Quadrant for 12 years in a row in the leadership area. We are one of the largest monitoring services provider today, MMS provider. We also kind of—we do a good amount of business in our threat intelligence because of our whole GIN, the Global Intelligence Network, and the capability that we have there. So strategies around expanding that portfolio to the incident response and the forensic services so that, you know, we are not just doing it in a proactive or (inaudible) but also reactive when there is a customer demand and then layer that with the security simulation services so that I can actually do better modeling and better preparedness and better health checks that are critical to this.

But just adding services is not adequate from a strategy perspective we realized. We also need to be able to scale up. There is a certain people intensive aspect associated with these set of services, but the more demand we actually take on and if it requires more people it's not actually something that you want to sustain from a margin perspective. We believe that more and more of this we can actually automate. So we're taking a lot of our incident response and other sets of offerings and we are doing a lot more technical IP development work there in order to automate more of this. We do streaming analytics, batch analytics, all based on the big data, an extremely fast way to really do these things such that the actual analyst that's actually looking at this is really doing more of the interpretation of the results versus actually having to go run a big query and wait four or five hours every time they have to do that. Same thing with data sets that they have to actually bring in and then constantly retain and archive and make sure that all of this is correlated on an ongoing basis.

So the technology aspect here in terms of the cyber security services is an extremely critical part of the puzzle here. But equally important is the customers are basically saying, "If I'm going to be running—I'm operating in Germany," or "I'm operating in Brazil," or "I'm operating in India. I want to be able to make sure that your capabilities are actually available to me while at the same time complying to the data residency and in the data regulation capabilities." So part of our strategy here is to expand our footprint from a global perspective to be able to really go after a larger geographic opportunity that exists there.

So, there are many differentiators here but in the interest of time what I'm going to do is to just walk you through each one of them very quickly here. On the security monitoring, as I said, one of our key differentiators is we have one of the largest shares in the market but we also actually, unlike other vendors in the managed services, we bring our own technical IP. Okay? The second, we also add on the IR and the simulation services in more of an end-to-end manner so you have a SOC where you're actually getting the service from us from a monitoring standpoint and then we have a team of people that actually can then work on IR type of engagement in a very flexible manner, emergency IR type option, retained IR type option, managed IR option, but more importantly they can take a lot of these things then, connect it to their monitoring service.

Remember what Jeff said earlier, if you hired—you know, when he was at Mandiant people would hire Mandiant, Mandiant would come in, react and respond quickly and then they leave and then the customer would say, "What do I do from this point on?" We don't leave them behind. We actually leave because we are connected into their monitoring capability, a lot of the tools that we use are actually now available for the SOC analyst that's actually working in the monitoring capability as well, so that from that point on after the breach happened for any new set of things they're actually using some of the same tools that we actually left behind because they're now part of our monitoring service as well.

We do this through a combination of, as I alluded to, a people as well as technology and this technology is an extremely important piece of the puzzle for us again. We cannot actually do this profitably and effectively and we can't scale this without some core tech IP. Analytics is a very important part of this and this is one of the reasons why it brings me to the next point that—actually before we talk about the next section, let me just talk very briefly about the revenue opportunities here. We have 100 self-monitoring customers today that are actually a tremendous opportunity for us to be able to grow and cross-sell our new IR services, simulation services as well as the threat intelligence. But with respect to the net new customers, we're also finding that we can actually provide some of these same capabilities but more from an end-to-end as opposed to somebody coming in and just looking at it from a monitoring standpoint. Between us and Dell SecureWorks or Verizon, they can actually look at us not just from a monitoring standpoint but monitoring IR simulation, etc. I think it gives us a differentiator in the net new install base. We have some very specific opportunities that we actually target in the public sector based on the agency requirements. Then as I said, the big growth opportunity for us is actually expansion into the new geographies to actually address the data residency issues and regulatory issues.

So, that brings me to this next part and that's a very important part of this puzzle that we are talking about, and that is how do we literally leverage this analytics that we—when we're talking about analytics here we're talking about a lot of the telemetry that we are generating from our threat protection solutions, information protection solutions as well as our monitoring and IR type of services. How do we really take that? How do we mine that, analyze that, create unique insights that not only help these other products and services that we just talked about but also how we can provide a lot of these insights in a self-service manner to the customers is something that we call our Unified Security Analytics platform. So I'd like to invite Amit Mital, who is our CTO, to talk about this and then I'll come back and talk about the go-to-market.

Amit Mital: Okay. Thanks, Balaji. Good morning. I think it's still morning. So as you've heard this morning from Mike, from Fran, from Jeff and now from Balaji, IT customers worldwide are suffering from this onslaught of attacks that are increasing in number, increasing in sophistication and frankly increasing in impact. This has been happening over the last several years. It seems like this trend is just accelerating everyday. We see this in the news. We hear it, we hear about breaches that are happening. We hear about companies that are compromised. What you're also hearing is that the existing technology and the existing approaches can't really keep up. They can't keep up because the methods are frankly reactive. There isn't enough data to educate IT about what is happening and why it's happening and where it came from and how to prevent it and as IT is trying to respond to these threats and respond to this onslaught of attacks increasingly they're chasing these false positives and so you have complete exhaustion based on all this time chasing

incidents or indicators which may or may not be happening. So what we believe needs to happen is we need to move from this manual process, which is very people intensive, where the false positive rate is too high and the false negative rate is too high, too many things are coming through, into a much more automated process where we can take the data and the visibility we have into what is happening across the industry, across the endpoints, across the control points that Balaji talked about, take the data and apply advanced analytics, advanced machine learning and automate that process because what we really need to do is dramatically reduce the latency, dramatically increase the accuracy and reduce the false positives.

Now, as you know, as of 2014, the average amount of time it took to find an advanced attack in an enterprise was over 200 days, which meant an advanced attack is sitting inside your IT environment for 200 days before you detect it. That is obviously not an acceptable situation that can keep going on and we need to find a different, a fundamentally different way of finding these attacks and finding them in a way that we can find them more quickly and more accurately and something that doesn't require as many people.

So this approach, this approach of automation, of massive automation is called Unified Security and this is our fundamental strategy for addressing this core security issue in the industry. What is Unified Security? So if you think about all this data that Mike talked about, the four trillion rows of threat information that we have in our database, the 200,000 new entries we get per second of everyday of every year, 200,000 new entries per second, that's a massive amount of information. This requires massive infrastructure at scale that can store this information, that can process it, that can analyze it, that can visualize it. So number one, what Unified Security is, is an infrastructure platform that allows you to store, analyze, visualize this information.

Next, what you need to do is take this information and do something useful with it. You need to allow IT and customers to make sense out of all this data, to do this cross-correlation that Balaji talked about, to find new threats, to visualize the data in different ways, to better—to do better risk assessments, to make better decisions about the environment, to find threats, to predict threats, to respond to threats. So Unified Security is also a set of applications.

Thirdly, and perhaps most importantly, the data we're talking about comes from many, many, many different sources. As you probably know, the IT—the security IT environment is extremely fragmented. There is no large customer that has a homogenous environment with respect to a vendor and so you need threat information from multiple sources, from multiple products, from multiple vendors. So what Unified Security also includes is a set of APIs that allows us to collect data not just from our own products but also from other vendors' products and this data can be accumulated either using—using either adapters that we use or adapters we provide and APIs we provide to vendors so that they too can contribute to our platform.

So what Unified Security really does is it brings all this data together into one place so that it can be analyzed both at the local level and the global level, it provides us platform so that you can bring together all this data in one place and analyze and visualize it and then do additional application on top. Then finally our hope is to provide a virtual cycle around this platform. What do I mean by this? These applications if you want to create on Unified Security aren't just applications that we create ourselves. We want to provide Unified Security as a platform to third party developers.

Why do we think this important? Well today as Balaji said one of the most critical issues facing people who are trying to create new security products is that the lifecycle or the time it takes to deploy a new endpoint, a new endpoint or in an enterprise can be up to two years. So let's say you're a startup and you say, "Okay, I've got this new, fancy new algorithm. I'll go to this finely-crafted network security and I have it the way of solving security for IT, for the enterprise." Well, it's very likely that you're going to spend the first two or three years of your life trying to get your endpoint technology deployed. Okay. So you can to begin with get access to the data. What we hope to do is say, "Look, we built this platform. We have a huge amount of data. We have more data than anybody else."

You heard Mike and Balaji and Jeff say we operate the largest civilian threat intelligence network on the planet. Well, we've got to process this data to developers so they can build interesting new applications and stand their IP and their IQ on top of our platform. As they build these applications, as customers buy these applications to generate more data this more data will make our applications even better and more accurate which will result in customers buying even more applications and it creates this virtual cycle and once that cycle start spinning we think it'll create a great differentiator for our customers and for us and for the industry.

So in a nutshell this is what the architecture looks like. Again, in the middle you'll see the infrastructure that I talked about. You'll see the data layer where we store data, global data that is anonymized across all our customer base but in also local data which is specific to each customer so that they can see information about their specific threat environment. On top of that is a services layer that allows you to do analytics and process the data in increasingly sophisticated ways and on top of that is the presentation layer so you can look at what this data actually means. On the top you'll see the applications that I referenced both first party applications and third party applications. Finally at the bottom you'll see the APIs, which allow us to gather the data from third parties and put them all together in one place.

So the fuel, the fuel that really drives the Unified Security platform is data. There's two critical parts of this fuel. It's not just the volume, and I've talked already about the huge amount of data we have, it's also diversity. You want as much diversity of data as possible. Why is that? Well you want to be able to look at a threat from as many different vantage points as possible. You want to see it from an email vantage point, from a network vantage point, from an endpoint vantage point, from the data center, from the cloud, from mobile. The reason for that is that in order to reduce the critical issue that faces security, the security industry today, which is false positives, you need as many ways of looking at the data and assimilating all the data together and saying "Okay, I can reduce false positives because I have verdicts from multiple places."

So imagine if a threat comes in, and I'm going to use the example that Balaji used where somebody tried to send me a piece of malware by email, and let's say the piece of malware somehow makes it into the IT environment because we didn't have enough confidence to convict the piece of—you know, the executable when it came in by email, but then we look at what it's doing on the endpoint and it's up to no good there and then we look at what it's doing in a data center. Now we have three different ways of looking at it and because we have different ways of looking at it and each of them seem suspect, we have much higher ability of convicting something like this malware. In many ways we are uniquely positioned in the industry to do this because we have market-leading positions across a very wide diversity of products. Not just one thing. We aren't just in the firewall, we aren't just in endpoints, we aren't just in the cloud, we are—our presence is across multiple places and we get to see threats from multiple vantage points.

So scale is super, super important and because of the scale and because of the data it enables a new class of applications that we believe will dramatically change the security landscape. Then as I mentioned, we also believe that it becomes an accelerant for innovation because now we can provide this platform. You know, we don't intend to keep this platform just to ourselves, we intend to provide this platform to third party developers as a platform for innovation and we believe we can create a virtual cycle around this innovation.

So in terms of how monetize, you know, obviously one of the ways is access to the platform itself and we could provide the data and the platform to our customers directly, but as I mentioned also to developers and as third party developers use this we believe there's a revenue opportunity for us to share in the revenue there. Also, we are going to incorporate the intelligence that we get from Unified Security into our existing products. So Unified Security will make our existing products even more effective. As we do that we think that'll have a dramatic revenue impact on existing products as well. So not only is that a new revenue opportunity, it also increases and amplifies and accelerates our existing product portfolio.

So I've talked about applications, I've talked about these applications we want to create on top of Unified Security. What are they? The first is a product called Cengage and Cengage is something that we will—we intend to release in the

next couple of months and basically think about Cengage as a way of benchmarking and analyzing risk across your enterprise. The next slide I'll go into more detail into what the scenario looks like. In an incident investigation you get to really drill down into incidents as they happen from a forensic basis. What happened, where did it come from, who's responsible, what other things are associated with this incident? Okay. Again, this is made possible because we have so much data. Okay? As Balaji said we get to record the data and go back in time and see what happened in history.

Similarly, we can do targeted attack detection. As in we can find and detect and identify indicators of compromise that result in attacks happening in customers worldwide. As we see these indicators of compromise in one customer, we then know what to look for in other customers. Okay? So this is an incredibly powerful capability and tool.

Then finally there's a product we're working on as well called Moneyball which allows us to correlate security outcomes among many, many, many different customers, which then allow us to go to customers and say, "We will enable you to make choices and trade offs between budget and risk profile and security deployment based on what you are comfortable with." So you could say given a fixed budget what different choices do I have to achieve a particular risk profile?

So let's talk about Cengage. Last year when we'd rolled the unified security strategy we really had three fundamental questions about the strategy. The first was how useful is the data? We have a huge amount of data and today we already use this data to drive, you know, many of the engines that underlie Norton and Symantec Endpoint Protection. So you already use this data in a very, very effective way today. But we really wanted to answer the question, what else can we do with this data? The second is, can we now analyze this data to find even more significant threats, these advanced threats that we keep hearing about? Then finally, what is the best way to monetize? What is the best way to monetize this analysis and this data?

So the way we decided to answer these questions was in the middle of last year we did this experiment. We called it the taste test and we did this experiment with a large bank, a very large bank and we happened to have a large amount of data associated with them. So over the course of several weeks we analyzed the data we had. We said, "What can we tell? What can we tell this bank about their security environment, about what is happening within their environment but also what is happening with their customers?"

As a result of our analysis, we found lots and lots of very, very interesting results. What we discovered was that there was targeted attacks happening within the environment as we did the analysis. We were able to figure out what is happening with these attacks, what is—who's causing them? What exploits were used to propagate these attacks? We were able to calculate a security ranking for this customer and help them understand how they were faring in comparison to their peers across the banking industry. When it came to their customers we were able to say things like, "Millions of your customers have been subject to phishing attacks to URLs that look very similar to yours." We were able to tell them things like, "A very large number of your customers have hygiene issues, computer hygiene issues for their mobile phones and their desktops." Okay? If you're a bank that is something of pretty significant concern because their credentials might be compromised. I recall the meeting I had in the fall last year with the (inaudible) of this bank and the two things that he said that still resonates with me. One, he was shocked with the data we presented, and number two, he said, "Look, I have a parade of security vendors come in through my office every week. I mean literally a parade and nobody can show me this information." That's a direct result of the vast amount of telemetry we have and coupled with the analysis that we did.

Now one challenge with the taste test was that it took a small team of people, a small team of our best engineers, the best security engineers we have, over six weeks to do this analysis. As you've heard today, these are people who are in incredibly short supply. You just can't hire them. Okay? There are literally just a few hundred of them on the planet, the people who can do this kind of analysis. We want—we think that this capability is so important that we want to make it available to our customers worldwide. Obviously this doesn't scale if it requires a small team six weeks to do the analysis for one customer and so of course the solution is to automate and there's one thing about my talk is about the

belief in automation as a cure for the general security issue that we face as an industry. If you'll recall at the end of last year we acquired the assets of Narus from Boeing and what the assets of Narus gave us most importantly was a large number of very talented security engineers with data analytics and machine-learning capability. So we promptly took those people and we are using them to automate the taste test and we really believe that this capability will drive dramatically new value for our customers.

Thank you, and I'm going to turn this over to Balaji. Thank you.

Balaji Yelamanchili: Is the mic on? Okay. All right. So I'm sure the most important question on your minds is, so when are all these things coming? We're talking about strategy, we're talking about specific applications and services, etc. As I said, the team that works on this is extremely passionate, extremely committed team; the developers, the engineers, the analysts and everybody else. They believe in this mission and when I wake up in the morning and come to work I come to work because of what they do and what they believe in. The kind of the focus that they have is actually about not just talking about the strategy, talking about the ideas but actually executing this. That's really what I'm really focused on at the end of the day.

To that end, what I wanted to do is to quickly share with you where we are with respect to the road map and then thereby how it actually can address or they manifest into specific revenue opportunities. What you'll see is we covered the threat protection and our strategy there and our offerings that we are working in, information protection same thing, cyber security services and so is this whole analytics platform and the associated applications. Over the course of the next 12 to 18 months what you're going to be seeing is a rapid set of releases and things that we're going to make available to the customers, whether that is in the context of the Advanced Threat Protection, in the context of information protection for the cloud and the mobile, expanded offerings from a cyber security services standpoint as well as the delivery of the platform and the analytics applications that Amit just talked about.

We also have, as Helyn mentioned, we want to be able to demonstrate a good portion of this to you, and so what we have done is during the reception hour after Mike and Thomas are done with their Q&A, during the reception hour we have actually set up three demo rooms where you can actually see the ATP in action, you can actually see our information protection and the Cloud Security Broker in action. You can also see Cengage that Amit very eloquently described on how powerful it is.

Obviously all of this is great but how do we really take it to the market? That's equally important. So we're very focused from a sales and a go-to-market perspective this 100% dedication. As Mike alluded to, the Enterprise Security Sales team is about 1,750 people and when they wake up in the morning and when they go to bed, in between all they're thinking about is enterprise security. They're not thinking about anything else. We believe that the focus will absolutely bring a good growth associated with that. We also believe that this particular organization needs to be very much enabled from a selling perspective, products, technology and the strategy, but also more feet on the street. So what we have done is over the course of the last six months or so as we're kind of preparing for the FY16 we have actually taken our Sales organization and looked at how to increase that quote-carrying capacity so much so that we now have the 40% more quota-carrying capacity within that same cost envelope that we're talking about.

We also believe fundamentally that we cannot go and sell point products to address the sophisticated needs that the customers have. We need to be able to do this in the context of the solutions and the services. That means connecting DLP with the Identities and Access Management. That means connecting ATP with the endpoint as well as the forensics and the remediation. That means taking the analytics platform and adding value to the rest of the products. That means that, you know, we need a lot more capability inside the Sales organization from a solution architecture and how do we really address that in the context of the customers' specific needs. As a result we are actually dramatically increasing the number of solution architectures versus the people that are focused on point products.

Then equally important is our coverage for the global key accounts where the majority of the spend is still a very important set of customers, the top 60 to 100 customers and they spend actually whether on us or anybody else they spend a lot of time and money in this and we want to get our share of the wallet, a fair share of the wallet and as a result we want to actually increase our coverage for these accounts and so we have actually taken our capacity and then improve the overall coverage there. Then we complement all these things through a combination of the partner and the channel ecosystem that's highly aligned to the kind of the strategy that we're talking about as well as the inside Sales organization that complements our commercial strategy in the context of the SaaS and the revenue and the subscriptions.

So that brings us to the story of the Enterprise Security as it relates to the FY16, where we are, where we're going and how we look at a lot of this. Obviously, you know, we're very bullish about it because of the new products and the new things that we're working on and then how it actually can tap into some of this expanded TAM. We also have—you know, we believe with the sales focus and the dedicated focus we have a very good increasing momentum. We have seen that over the last six months and we expect to actually build on that. We have tremendous assets that I talked about both in terms of the presence that we have at the control points, the telemetry that we have as well as the technologies that we have that we can use to innovate but it is about the execution that's the most important thing here and then we have a strong install base that we can actually leverage from.

So what I would like to do is to invite up Jeff and Amit for about 10-plus minutes of Q&A, and then I guess break for lunch.

Jeff Scheel: Oh, I'll take this. Thank you. All right.

Helyn Corcos: We're ready to take our first question. We're going take Steve right here. Thank you.

Steve Ashley: Oh, thank you. Steve Ashley, Robert Baird. I have a question I need to repeat. Is that a offering that will sit behind third party products if someone is using a third party email product on the front line? Is that something that you'll be able to work with and how should we think about that?

Balaji Yelamanchili: Yes. So the question is whether or not actually it works with a third party. When you talk about the third party from an email provider, yes we work with an email provider. If your question is whether we work with a third party email security provider, the answer is no. We actually do that in the context of our email security service as well as our endpoint capability. But on the network side in addition to our own network sensor we also work with the other network sensors including the likes of the Palo Alto and WildFire.

Yes?

Helyn Corcos: We'll take—Sean, we'll take a question from Walter.

Walter Pritchard: Thanks. Two questions. One as it relates to just hiring people in this space, I mean you talked about Narus bringing you some good talented engineers. Are you—I'm curious, who are you hiring at this point? What types of people are they? It seems like a really competitive labor market in the security space in general. Are you sort of biting the bullet and just paying more for people given what seems like some inflation in that space or I'm curious what strategy you're employing there? Then from an acquisition perspective, I mean I see a really rich product road map. It doesn't seem like—Narus sounds like almost an Apple hire, a diamond in the rough so to speak. It doesn't seem like the message here is we need to go out and buy a lot of security technologies to bolster the portfolio. I just wanted to hear commentary around how you're thinking about acquisitions in the enterprise security space.

Balaji Yelamanchili: Okay. So there are obviously two questions. I'll try to answer the first one and then we'll come to the second one as well. So as it relates to the talent, the talent is just—it's certainly on the engineering side more and

more the analytics experience and then the ability to do that within the context of the security domain is extremely important. Narus is a perfect example of why we became very—we decided to be very opportunistic and do that and thereby increase that. But we certainly see that as a critical part of the puzzle. We are very focused on doing the right thing from the standpoint of the acquisition of that talent. Part of it is where the talent is and hiring that. Part of it is also making sure that, you know, from—it's not all about the compensation, it's also about the mission focus. What we find is many people are attracted to this industry because of the noble nature of what this is all about and we certainly tap into that and we actually find ourselves in a good place. Then we have the brand name and the recognition that actually allows us to hire the best talent. So we obviously, you know, take full advantage of all those things in addition to all the other traditional approaches to go after the talent.

As far as the acquisitions, I think Mike...

Michael Brown: Actually I wonder it might be interesting, Amit, could you add to that because you've actually helped us upgrade a lot of the talent especially in what we call STAR organization, or Security Threat and Response, so I think your perspective would be helpful there too.

Amit Mital: Sure. Thank you Mike. I'll echo what Balaji said. I think—well there's a couple of things that we have really internalized in building the technical talent within our organization. Number one, security is such a dynamic field and its moving so fast and is so competitive that you really, really, really need to hire the best talent and you can't really compromise. In my experience what I found is that great engineers care about really two things. They want to work on great stuff and really impactful things and they want to work with great people, okay, which further reinforces the fact that you need to really have a high, high bar. So in the past year our focus really has been on number one better articulating our mission and focusing our strategy so that—even more exciting and compelling so that we can attract the best talent, but at the same time, raising our bar so that when we do hire people—you know, we don't hire people saying, "Hey, I just need a guy and I need him for a month or two months." We hire people who have exceptional talent and never compromising on that. So as a result in some of our core security organizations we've turned over the organization by about 40% and it's been hard to do but we've had a relentless focus. Most of my leaders in my organization spend nearly 30% of their time on recruiting and hiring, which, by the way, I think is the appropriate level.

Helyn Corcos: Sean, Mike has a question on the end (phon).

Michael Brown: I don't think we answered that. (Inaudible) about...

Balaji Yelamanchili: Yes, a second question...

Michael Brown: ... about (inaudible).

Balaji Yelamanchili: Would you like to answer that?

Michael Brown: Okay, sure. The security industry as we know is very fragmented and that's because of the new technologies (inaudible) the new threats, so we're very aware of that. Symantec as we all know is built on a history of acquisitions. For the last few years we've been out of that market. That wasn't what we were doing under my predecessor but we don't think that's the right approach. Narus is an example of seeing something that was obvious for us. Now that we have clarified what the strategy is, you can see the amount of effort we've put into saying, "Here's what we need to go do," and with the clarity of that mission now it becomes clear what makes sense for us to think about, because you could spend all the money that Thomas counts, and more, buying up stuff that might not relate to each other—not more—and then you just have more point products that customers become frustrated with. Frankly, in our history, if we're critical, we've done that a few times. We're not doing that again. So, you can see very clearly we're going to be active, but we need to have something that fits quite concretely with what Balaji and Amit described here as

fitting in. Threat protection, information protection, adding capability to services, or helping us build that unified security analytics platform, we are now very active in looking at what makes sense in that market.

Michael Turits: Hi, it's Michael Turits from Raymond James. On endpoint, there's been a lot of discussion about shifting the budget dollars from so-called traditional input, where obviously you're a dominant player, to—let's call it next-generation endpoint, which includes a lot of the solutions you've talked about, in terms of forensics, protection, et cetera. So, what's your self-confidence that by making these investments you can expand your addressable market and your revenues in endpoint, as opposed to just supporting or bolstering that existing revenue base?

Balaji Yelamanchili: Would you like to take that, Jeff, first and then I'll add to it?

Jeff Scheel: Yes. I think that the most important thing is to really look past the rhetoric kind of in the market and look at what the install base looks like, and the capabilities, as Balaji pointed out, that already exist, and in some cases what's happened is we've got customers who aren't fully utilizing all of the capabilities that they've deployed, and one of the things that the—the ATP solution, for example, is going to unlock a relationship between all the actionable intelligence we have and their ability to make use of it on the endpoint. So, that's the first thing.

The other thing is we are looking at—as Mike indicated, we're looking at things that would supplement our ability to do, basically, detection and response more effectively, because the way market—so one of the other areas I cover is our analyst relations, so Gartner and so forth. The way that Gartner characterizes the endpoint market is they talk about protection, detection, response and prediction, and historically, we've been in the protection marketplace and we've been a leader there, but in a world where compromise is inevitable—and customers are starting to realize that—it's all about how quickly you detect and respond so that you don't end up with a breach. So, compromise does not equal a breach. Compromise is going to happen all the time. It's inevitable.

One of the big banks that we work with, very locked-down policies, guess what? The Russian mob decided that they would get in a different way, by targeting the country club where they all belonged, and so when the next PDF came in from the local country club, every one of them opened it and launched 17 different kinds of malware.

So, what we're looking at are what are other capabilities that we can add that keep us current and enable us to do better detection, and then response, as quickly as possible?

Helyn Corcos: We have one more question here in the back.

Matt Hedberg: Yes, thanks for taking my question. Matt Hedberg, RBC. I'm curious if you can give us some more details on the go-to-market strategy of your email archiving backup, and then the email security business, if the pending split of—or IPO of Veritas changes that any way, just I guess thinking about the archiving and backup versus the email security side, which oftentimes go hand-n-love.

Jeff Scheel: Mike, would you like to take that?

Michael Brown: If you can repeat the question, we might want to get Matt …

Jeff Scheel: The question is—when it comes to the email, there are two distinct offerings, Symantec, larger company, one is the email security and the other one is the email archiving. With the split, how is that going to manifest?

Michael Brown: Well, it does go with the two separate businesses? So, maybe I'm missing something …

Matt Cain: I think the question is—I think perhaps your question is around security for the archiving?

Matt Hedberg: Yes, I guess I'm wondering—it's two different businesses and they oftentimes go together. Does that change sort of how you address that sort of joint market?

Matt Cain: (Inaudible) and what we do with email security, so we didn't even, from a go-to-market perspective—before when were combined Symantec and Veritas, there wasn't a joint go-to-market strategy there at the combined company, so we wouldn't see it as a separated company.

Jeff Scheel: There are a few areas—to generalize that a little bit—there are a couple of areas where we do see more synergy, and so what we're contemplating is the right level of cross-selling agreements that make sense. As Brett indicated, there aren't very many of those that kind of speak to the strategy and the separation, but where they do exist, we want to make sure that we're maximizing the opportunity for both Symantec and Veritas to go forward. We've got a pretty good handle on what those are from what synergies we did see already in this period. Where we have two dedicated focused sales forces, Brett and his counterpart, Adrian Jones, already working, to make sure we maximize that. So, where it does exist, we want to make sure we take advantage of that opportunity and we'll set up the right arrangements as we're two independent companies for that to work well.

Helyn Corcos: Okay, thank you. So, now we're at the time where we're going to take our 15-minute break and grab some lunch. Also, if you're interested in seeing any of the demos, we have three that we're going to be presenting this afternoon during the reception; please sign up at the registration desk. There's going to be one on advanced threat protection, one on information protection, and then another one on the security analytics platform, or SYMGAUGE, the actual solution. Thank you.

(Lunch break)

Helyn Corcos: Good afternoon. We are about ready to resume the last portion of our event today, and with no further ado, I would like to introduce to you our CFO, Mr. Thomas Seifert.

Thomas Seifert: Thank you, Helyn, and I'd like say good afternoon, too. You heard a lot of exciting stories and by now you're probably wonder how is that all going to impact the numbers moving forward, and this is what I'm about to talk to you about, and since Mike is not here I have a large degree of freedom to improvise now. Oh, here he comes, so I have to be careful.

So, I'm going to cover a couple of topics. I want to set it off with what we've achieved in fiscal year '15, and then really go into specifics for each segment and how we look at the path to growth in the year '16 and '17, what that means to cash flow, and at the end really cover—and I'm going to give you an update on where we are in the separation process and also where our restructuring efforts are.

So, if we want to talk about what we have in front of us and how do we get confident in us accelerating growth, increasing profitability, and how the numbers are changing, then we really have to tell the story in three chapters: our focus in '15, acceleration in '16, and then really unlocking value in '17. I think it's fair to say we came along way in '15. Focus allowed us returning to growth, we right-sized the cost structure of the Company, we hit our profitability targets, and at the same time we have been able to shift significant R&D dollars to market segments that are growing fast, that are attractive, and that prepared the pipeline by Balaji and Amit and John and Matt have been talking about. So, we take a lot of momentum of what we has been laid as a foundation into fiscal year '16, our current year. That allows us to continue to build margin, as you will see, we will deliver the product roadmaps that have been presented to you on top of that momentum, and of course we have to separate the two companies, and then really getting into fiscal year '17, we will look at two streamlined businesses that are both on an accelerated growth path, that deliver improved margins, and will deliver, as you will see, significant cash flow moving forward.

So, let's just capture what the foundation was that we have laid in fiscal year '15. So, I think it's fair to say we turned a corner from a growth perspective. Our deferred revenue growth is up year-over-year significantly, recovering ourselves out of the hole we were in. The same is true for implied billings growth. Those leading indicators, when it comes to revenue, are really important, because during a quarter only about 25% of the bookings we achieve are really turning into in-quarter revenue; 75% of our in-quarter revenue comes off the balance sheet. So, that's why you'll have to look at some long lead time indicators on revenue development. The good news is, however, if you look at fiscal year '16, close to 50% of the revenue that we have achieved is already on the balance sheet, and we have achieved our profitability targets and hit our 30% mark in the third quarter. That is good momentum that we will take into fiscal year '16 and '17. For sure, there will be some seasonality around it, as you will see, but the run rate is in the right zone.

We have been able to achieve that because we have been rather successful executing on the eight initiatives that we outlined last year, four targeted on top line, as you remember, and four targeted around the cost structure. They helped us to achieve $150 million of margin dollars in fiscal year '15, but more important, we take about $225 million, $230 million of run rate with us into fiscal year '16, so that is great momentum, and it allows us, on three of those eight, renewals and pricing and up-sell capability, to build even momentum on top of that. So great foundations, and let's not forget we have delivered on those improvements while we were executing a rather complex separation.

So, as you heard today and heard before, we made a strategic decision to separate the security and the IM business, really trying to gain focus and strategic flexibility, reducing operational complexity, and you will see this really reflected in the numbers, and really enable each business to take advantage of its full growth potential in their respective market segments.

So now, I would like to take all of those three segments each by each and describe and discuss our path to growth for each of those segments. So, let's start with Veritas.

So, Veritas came a long way. You saw this already in John and Matt's presentation. We increased our margin by 12 percentage points over the last three quarters, hitting a 25% operating margin in Q3 of last fiscal year, fiscal year '15, and we accelerated the business already from a revenue growth perspective to 5% in fiscal year '15. So, a lot of momentum that helps us getting into fiscal year '16, and in fiscal year '16 we launch a whole slate of products that Matt has been talking about, and you heard him also talk about we think this is the healthiest product pipeline we have in a long time and we have the high confidence to deliver this product along this time line.

So, what does it mean? For the IM business, for Veritas business, for fiscal year '16, we guide revenue in the range of 4% to 7%, and we will continue to take the momentum we have on the margin side with us into fiscal year '16, guiding for a range of 27% to 29% in fiscal year '16 for the Veritas business. Entering in '17, we see this momentum continuing. We think there is further room to improve the margin, mainly driven by the new products that are coming in, but also the progress we see on accelerating our sales productivity. When we come to the restructuring numbers, you also see that. John and Matt and the team have spent a really good job taking advantage of this separation and simplifying the business model in a major way and taking some of the complexities away that were built up over time by just trying to keep two businesses together from a go-to-market perspective that really don't belong together. So, with this momentum, we see revenue growth in the range of 5% to 8% for the Veritas business as a target in fiscal year '17, and we will see the margin target in a corridor of 29% to 30%. So, so much for the Veritas business.

The next segment is the consumer security segment and here the focus is really on stemming the revenue decline, and you heard Fran talk a lot about what is in flight, but if we go back to fiscal year '15, we started the fiscal year '15 really with forming a business unit at the beginning of the year, and Fran and his team really embarked on a massive business implication and cost reduction, also exiting unprofitable market segments, and this really helped us to expand operating margin by a thousand basis points, a really respectable achievement.

So, we are confident that there's enough productivity in the business over the next two years that we can keep the margin stable despite the revenues declines—you heard Fran talk about this already—but then we have a whole flight of actions in place that Fran talked about that help us mitigate the revenue decline in a major way. We moved to a single-subscription service, we are expanding our merchandising flexibility, and Fran spent a lot of time talking really about how we enhanced the customer experience. So, lots of small operational steps that are going to add up, but we target to get revenue decline in fiscal year '16 in the range of minus 5% to minus 8%, and as I said before, keeping the margins stable in the range of 52% to 54%. So, the decline is going to be reduced further. You heard Fran talk about how much lead some of the measures have that he has started to implicate. So, we look at a range of minus 3% to minus 6% in fiscal '17—that is how Fran got to his midpoint of 4.5% that he talked about before—and as I said before, keeping the margin stable around 53%, at the midpoint, between 51% and 55%. So, this will help us to continue to generate significant cash flow that we are able to use to fund the buildup in the growth of our enterprise security business.

The enterprise security business in '15 was really all about getting the product pipeline ready for '16. So, we spent a lot of time—less time on the enterprise security segment right-sizing the cost structure, but really shifting R&D dollars to products and product development where we see a lot of benefit, and fiscal year '16 is then the first year where we see the fruits of those efforts. Balaji and Amit spent a lot of time trying to explain how the new offerings around advanced threat protection protects, around their cyber security services, and the unified security offerings, when they hit the market. The important part is really that not only do they attract highly interesting markets from a growth perspective, they allow us to open the addressable markets for us in a significant way, 50% for both the security services, as well as the ATP product, and ramping those products in the second half will mean for us that we can target a revenue growth range of 1% to 6% for enterprise security products in fiscal year '16.

Margin will be under slight pressure in fiscal year '16, in the range of 10% to 12%, primarily for two reasons. First of all, we have focused on R&D to make sure we hit the product launch dates, and it's also the fact that the enterprise service products, the security service products are ramping a little bit faster and earlier than the ATP and the information protection products, and that is, at least in the beginning of the year, a little bit dilutive to our margin efforts, but a significantly picked-up run rate from a revenue perspective for enterprise security in the second half getting us to a range of 1% to 6% for revenue growth in fiscal year '16.

'17 is for us all about catching up with market growth. We'll take full potential of the run rate of the new products that have been launched, and there will be of course additional products around the analytics platform that are going to be brought to market in '17 and monetized, but we target a revenue growth in the range of 6% to 10% for enterprise security products in fiscal year '17, and a margin increase. So, the product mix is catching up with us and some streamlining that we will initiate in the latter half of fiscal year '16 that allows us to get the margin for the enterprise security business in the range of 14.5% to 16.5% in fiscal year '17.

So, these are the three segments. So, how does it all add up? Because we have to look at—before I get there, let me make one more point.

So, the enterprise security growth path is of course driven by the new products that we launch, but, similar to the Veritas business, they are not the only lever we have to get to revenue in the enterprise security business. We're in an extremely great position to create growth through monetizing really our unique assets, the strong foothold we have from a install base perspective in endpoint, in data protection, and also in our security products, and really taking advantage of our enterprise security franchise, really monetizing the telemetry that Amit has been talking about, and this opportunity is significant and it's very tangible for us because it needs only small improvements in those levers. So, what do I mean by that?

When we say there are seven products in fiscal year '16 that allow us to expand our addressable market, what does that mean? Every 100 basis points of new market TAM that we open up over three years give us a $350 million revenue opportunity. So we launched seven new products in that space, and we launched those products, as you heard from

Balaji, through a much more optimized, highly efficient go-to-market engine, both from a feet-on-the-street perspective, as well as the number of quota-carrying folks we have, and so on, so significant opportunity. But beyond new business, the operational levers that we have are continuing to be super interesting.

So, we worked on retention already as one of our eight initiatives in last fiscal year, and we set up a dedicated renewal organization. There is more potential to go after. We have an $800 million renewal opportunity every year that allows a lot of upside for us, and if we look at the leading—industry-leading likelihood to renew, compared to all of our competitors—so not only is the renewal opportunity for us significant, we also have a high likelihood that customers want to renew with us.

Pricing continues to be a very important lever for us. A 100-basis point pricing improvement, we've seen this already in fiscal year '15, at about $100 million of top line performance, and since this is almost exclusively profit, it adds about 200 to 300 basis points to the operating margin.

The largest lever we have in '16, based on the new products we launch, is really our up-sell and cross-sell opportunities. So when you go into demo sessions after and Mike's and my Q&A session, I really would like to ask you to look at the products not only from a pure performance perspective, because that is exciting, but the opportunity those products have to either up-sell in the ATP or in the information protection case, or to cross-sell if you're looking at a product like SYMGAUGE. Our large install customer base is one of the biggest assets we have. If we follow internal statistics, we have a five times higher likelihood to sell to an existing customer new product than we have attracting a new customer. so really turning this into a new business is important. Just to look at that, the customer base is large. The opportunity to add one product, new product to all of the customers we have is a $1 billion revenue opportunity we can go after. So not only are the new product important, that's why we are energized by being able to complete really the redesign of the go-to-market efforts and being focused and dedicated, and having more feet on the street.

So, with that said, how is everything going to add up? We talked about the three segments in detail. How is it all going to roll up? So in '16, the numbers that you are going to look at represent a pro forma statement of what Symantec is today. So those numbers include the Veritas business, they include the Norton consumer business and the enterprise security business because this is pretty much what Symantec is going to look like at least for the first three quarters of this. So for the combined company, we look at revenue growth in the range of flat to up 2%. As we said before, we are taking a lot of the margin momentum, both on Norton but as well as the expanding margin opportunity on the Veritas side, with us, so operating margin in the range of 29% to 30%, and we will also put some EPS growth on top of the performance we have for fiscal year '15. We expect EPS to go up between 8% to 14%.

For '17, we have left the pro forma number on top, but this entity up there doesn't really exist anymore in '17, so it's really important to look at the individual elements. We already went through the Veritas numbers for fiscal year '17, revenue in the range of 5% to 8% and operating margin in the range of 29% to 30%, and then just to make sure we talk the right Symantec, Symantec security, which is the add-up of the Norton business and the enterprise security business, in the revenue range 1% to 4%, so we see growth not only for enterprise security, but for the combined Symantec security entity, and an operating margin that moves us in the zone of 30% to 30%.

So, overall, if you keep the pro forma numbers in fiscal year '17 in mind, the 300 basis points of operating margin expansion, so continued expansion, and we are returning to growth, and if you return to growth and increase your margins, that normally means good things for cash flow. So, cash flow from operations, we expect to come in around $1.3 billion in fiscal year '15. We think we can increase this by about 12%, despite the fact that we are separating the companies in fiscal year '16, to $1.5 billion, and then really continued margin momentum and accelerated growth getting us to $1.8 billion in fiscal year '17, about 26% up compared to the previous fiscal year. The split is slightly north of $1 billion for Symantec and slightly south of $800 million for Veritas in the fiscal year, and of course this allows, once the companies are separated, for two very interesting businesses and entities from a capital distribution perspective.

That's actually a good turn into the next segment. So, what do we do? So, here is where we are on capital allocation at this point. If you look back on our history, we have constantly paid more than 50% of our free cash flow to shareholders. We're getting to the $900 million in fiscal year '15 that we have been promising. The Board, in the meantime, in February also approved a further $1 billion share repurchase program. So until the separation, which is going to happen from a legal date perspective—you'll see this in a minute—on January 2nd of next calendar year, we are going to continue to return both cash dividends and buybacks at the same level as in fiscal year '15, until we reach the separation date, and then post separation we can be more specific around Symantec, so we will continue for the Symantec business to pay attractive dividend yield and continue with our share repurchase program.

On the Veritas side, I have to ask you for a little bit more patience. The cash flow generation, as you saw, is really good, but we will provide more detail on what we do with this cash—there are many options—when we come closer to filing our Form 10 in the summer of this year, not too far away.

So, we talked a lot about separation in Mike's section and in my section today. It's about time that we give you an update on where we are. So we are on track to separate Veritas and stand it up as a very attractive standalone business. We reached a very important milestone at the beginning of this fiscal year. Our new fiscal year started on April 4. So the sales force is already separated. So all the productivity numbers you saw dedicated to Veritas, dedicated Symantec teams, higher rate of quota-carrying reps, is all in place, and that's what's very important to us, that we do not impact the momentum we have and disrupt the momentum we have from a go-to-market perspective in fiscal year '16, while we separate the companies. So we put a lot of upfront effort making sure that their teams are stood up, not only in North America but globally, that the quotas are in place, the sales incentives are in place, that the coverage models are defined, that the key account structures are set up, and as I said, we achieved this date—we started the new fiscal year on April 4 with a separated sales force.

The next key milestone that we are aiming for is filing our Form 10. We foresee that in the July timeframe this year. It will be followed then by the credit rating agency discussions that we have. Then, we target operational separation on October 3 of this year. So, we will have one quarter trial and testing until the legal separation happens then on January 2 of next calendar year, and you heard from Helyn this morning that the first day of trading would be January 4 for Veritas as a separate public company.

We increased our expected separation cost range to about—into a range of $170 million to $190 million; that's up quite a bit. It's primarily driven by a higher degree of complexity separating the IT infrastructure, to be honest. So it's higher costs but we are very confident around the timeline, separating the IT infrastructure not only from a network, but also from a data center, and even more importantly, from an enterprise application perspective. It's a little more complex and requires more resources to get the work done and that's why costs came up.

We also increased our range for restructuring costs into a range of $165 million to $195 million, and this is really taking advantage of the opportunity we see to further streamline the organizations moving forward. So, we see further opportunity to be more aggressive putting the new entities into a smaller footprint, from a number of locations perspective, from a number of legal entities perspective, streamlining the processes and taking costs out, and it also includes a higher restructuring number on the employee side. You might remember that in December we announced a reduction in (inaudible) program that affected or should have affected about 10% of our employees, 2,000. With the new measures that are in place, we are aiming for a number that is quite significantly north of that number, and it's also a part of the reason why we are confident that we have pretty streamlined organizations in place, and that's why we are not so nervous about the synergies that might happen from a separation perspective, we think we have enough buffer to compensate for that.

So, with this all being said, let me try to summarize the day and my presentation. We think we have come a long way. Focus drove us returning to growth from a billings and from a deferred revenue perspective, and hitting really our profitability targets in fiscal year '15. We're going to build on this momentum to accelerate both margin expansion, as

well as growth, both for the Veritas, as well as for the enterprise security business, so a lot of operational levers, but especially through launching new offerings that in both businesses significantly open up our addressable markets.

We are on track to separate Veritas as a standalone, a very attractive standalone business, and based on the initiatives that are in flight, we think we have two streamlined businesses moving forward that grow on a more efficient cost base and will deliver significant cash flow, and with that, EPS improvement forward, and we as a team, all the people you saw today up here and in the room, we are committed to unlock value and continue to return cash to our shareholders.

Thank you.

Helyn Corcos: Nate, if you can get Phil back here. Thank you.

Philip Winslow: Hi guys. Phil Winslow, Credit Suisse. Just two questions. First, Thomas, I just want to make sure I heard you correctly that the reason the restructuring number is higher is because you're going greater than 10% …

Thomas Seifert: Yes.

Philip Winslow: Is that what you meant? Okay.

Thomas Seifert: Yes.

Philip Winslow: Then do you have a feel for kind of what that percentage is? Then second question: obviously, there's was speculation about a week ago that you guys were in substantial negotiations for the Veritas sale. Obviously, there are a lot of Safe Harbors in Section 355(e) of the Internal Revenue Code as far as that a second transaction could occur with Veritas post spin. Some of those could be six months or it could be up to two years. So the question is did anything happen over the past few months that would violate any of those—or break any of those Safe Harbors, I guess. So, two questions.

Thomas Seifert: So, the first question was, remind me—I was so focused on your second one.

Philip Winslow: What the percentage actually was? It was greater than 10%, was it 12 …

Thomas Seifert: Yes. So, we're going to be north of 2,500.

Philip Winslow: Then the tax Safe Harbor.

Thomas Seifert: That is still in place. That's our standard regulation. A change of control event could not happen in a timeframe anywhere between six months to two years, depending on how severe and intensive the discussions were that happened before a separation takes place. So, that ruling is in place.

The second part of your question would assume that I answer the rumor first, and since we never comment on rumors, I'm not going to talk about the second part. I mean we said in the beginning that we are very diligent about how we look at this. We work on the separation with a spin, because this is the timeline we control. It's quite a lot of work. It takes a lot of Management attention to go through a separation, so you try—and keeping the business momentum at the same time. So we don't want to make life too difficult for ourselves, either. We try to protect as many decrees of freedom as possible moving forward.

Michael Brown: Yes, just to add to that, the key thing from a strategic standpoint is the separation. We're clearly focused on that. As Thomas said, the public spin is within our control. We remain focused on that. If we receive some serious interest in between, the Board understands the trade-offs, the right thing to do for the shareholders, which

would take into account how serious, what the price is, what the after-tax implications are, and so forth. But as a public company, obviously we can't comment on what's happening or what's happening along the way, so we remain focused on the public spin option. That's with the timeline that we committed to today is all about.

Helyn Corcos: Great. A question from Brad.

Brad Zelnick: Thank you. Brad Zelnick with Jefferies. Just a particular point. As you're speaking, there are additional headlines breaking around what sounds to be a parallel process, and we appreciate that the focus is on the spin which you can control the timing of, but just specifically, either outcome, there's the question of what the tax basis is of the Veritas business, and regardless of whether that's ultimately deferred to the shareholder or, you know, something that the core Symantec business needs to pays tax on. Can you just speak to what that basis is, or how we should think about that?

Thomas Seifert: I'm not aware of the headlines. We're too busy here, but I was just told it's a resurfacing of the old news, so it's not really new news. Of course, as part of the separation, we have to look at tax bases in detail to understand where we are. There are many opinions out in the market that it's very low, down to zero. That's not correct. It's not zero but it's not too high, either; it's south of $1 billion, and that needs to be considered moving forward, making sure that we have the best interests of our shareholders in mind.

Helyn Corcos: Next question? We're going to go with Mike and then we'll go with Keith.

Mike Turits: Thanks. Just a question on cash flow, especially since you're raising those restructuring and separation charges. You've got cash flow going up by about $200 million. So, it looks like a high bar to hit on cash flow. Does CFFO exclude these charges or not?

Thomas Seifert: CFFO includes separation and restructuring charges. These charges span between FY15 and FY16.

Mike: Okay.

Helyn Corcos: We have a question in the back here with Keith.

Keith Weiss: Thank you guys for the presentation. In terms of cost cuts, you're upping the level of restructuring to almost 2,500 employees. It also sounds like you guys are hiring pretty aggressively, building on your businesses. So a couple of questions. Can you just give us the timeframes? Because I thought I saw different data points in the presentation. The expansion you're talking about in quota-carrying sales heads, 20% on the Veritas side, 40%, has that happened already, has that …

Thomas Seifert: So, a good point. It's probably important for us to make sure that we make the point. I think John hit it in his part of the presentation. So, the changes in the go-to-market are within 100% move, so we are not adding people. Actually on the Veritas side, we take the overall go-to-market cost envelop down, targeting for 25% of revenue, but within the sales and marketing spend, we are reallocating dollars and we are increasing the number of folks and feet on the street, and taking down management layers, co-ordination layers, and really, you know, it gives you, in part, an indicator of the cost of complexity of keeping two businesses together that really didn't belong together anymore from a go-to-market perspective. So, this happens on the go-to-market side where we are really—so we hire and transform within the spend, and where we really hire people and—Amit, I think, made a good point on how focused we are on engineering and development resources, but, still, the overall footprint of both entities is going to shrink.

I think in one of the first meetings Mike and I had, we talked about the number of locations we have worldwide, how many legal entities we support, and data centers we have, and we just take advantage of this opportunity of the

separation to clean this up. Halfway through the separation, we just discovered that there are more opportunities than we thought and we want to make sure that we take advantage of that process.

Keith Weiss: Got it. So the 2,500 number, is that a net number? Is that net headcount reductions? Or is it a growth number that you're going to hire on 1,000 people in cyber security or in sales and actually cut down 3,500, or something in that delta?

Thomas Seifert: So, will all of the reductions drop down? Probably not. But the reductions that we just announced in the restructuring costs are reflected in the guidance we gave, and of course I impart it's only a part of the reason why we have margin expansion moving forward. So, they are reflected in the numbers that we just outlined.

Michael Brown: But, to your point, Keith, we are hiring in a number of areas even though we're cutting others. So there's a big skills mix rebalancing going on, again, to make sure that we're addressing the higher growth markets, that we're shifting our resources there, shifting in R&D, and as we talked about with sales and go-to-market, some of the same thing is happening there.

The changes that we talked about on go-to-market in the two focused, dedicated organizations were effective as of two weeks ago. So I compliment both Brett and Adrian in terms of having what we call fast-start. So some of the training, some of the work with their management teams began months ago in terms of planning this. Both organizations have worldwide sales meetings, two separate sales meetings that will happen a week from now, to make sure everyone is completely trained, but everyone already has the new management train in place, quotas, territories. That was already to go as of two weeks ago when we began it, and that's a lot faster than it happened last year without the separation. We've already had an all-employee meeting to share what the Company goals are for the year. That started the second day of the fiscal year. So, people are already very well informed and ready to go. I'm very pleased with the focus that we're achieving and the fast start on FY16.

Keith Weiss: One last one on the gross margin line. You guys are talking appliances are growing really well, you're talking about more cloud services and more sort of human capital services and more consulting services. What should our expectations be on gross margins on a going-forward basis with some of those—what we think of as lower gross margin businesses ramping up as a percentage of the mix?

Thomas Seifert: As we move forward, we will give quarterly guidance that takes also more product mix information into account, but as part of that margin expansion, you have headwinds and tailwinds. So headwinds for sure are a higher share of appliance products. Also, price points are changing, because you heard from Matt that we address with the new appliances that are coming up a completely new market segment. So, it's more differentiated than saying just appliances are dilutive and the rest is not. So the mix is normally pressured from a faster ramp on the appliance side, but, however, the pressure becomes less as we target different segments. The new products beyond appliances that we launch will be part of our ability to increase margins, supported with the continued restructuring and streamlining we have for that business. This is really one of the unique advantages of standing up Veritas as a separate company. As part of the separation process, we are able to redesign a couple of our core processes in a very significant way and take a lot of complexity our, you know, where the Veritas business was just burdened with stuff from security go-to-markets that are not needed.

Michael Brown: Maybe just to add a little bit on services, since you touched on that and that's a key growth area that Balaji highlighted. The services margin, as you might expect, is different depending on what kind of service you're offering, too. So, monitored service has traditionally been lower margin. Incident response, actually, is quite high margin. So, there's a mix going on, obviously, as we expand that full range of services to how much capacity do we invest in each one, we're going to be planning that as a business model as that becomes a bigger part of our business, and as Balaji importantly said, was not just a people-oriented business—our view of services is the way we get better and actually provide better service for our customers is applying more technology and automation to the service

offering. So that's key to our thinking about how to grow a very profitable services offering. We'll be sharing more about that as that evolves over the course of the year.

Keith Weiss: Thank you.

Helyn Corcos: Great. We have a question right here.

Fatima Boolani: Hi, it's Fatima from UBS. I'm wondering if you can comment on the cap ex profile of the businesses coming into next year, and then a year out. You've taken a lot of steps in consolidating your infrastructure footprint through fiscal '15. So, I just wanted to get a sense of what that would like, especially as you build out your service security capabilities and are perhaps making that stand to carry the operation centers worldwide.

Thomas Seifert: Yes. So, for fiscal year '15, we're running about at a rate of $400 million of cap ex for the combined company. We always said it would be about $100 million above our normal run rate, because it already included a significant investment getting a cloud-computing platform ready for the new products that we are talking about today. For fiscal year '16, it's going to be in the same neighborhood for the combined company, $400 million, around $400 million, but $100 million in this $400 million are really just cap ex driven by the separation, so our run rate is going to come down, actually, our normal operational run rate is coming down about $100 million of separation. So, I would say 300 is about the right run rate number for the combined company. I don't want to go into cap ex guidance now beyond '16, as that is too early, but I think it's important to understand that from an operational perspective, cap ex is already normalizing this year.

Helyn Corcos: Great. Another question right here.

Matt Niknam: Thanks. Matt Niknam from Goldman Sachs. Just a question on Veritas. You've talked about margin expansion over the course of '16 and '17. I'm trying to understand specifically in '17, once this is its own business, does that capture any sort of G&A, corporate overhead, you know, which typically comes with these types of spins?

Thomas Seifert: Yes, it does, and actually the overhead needs to be already in place in '16, otherwise it would be really difficult to spin the company. So, that's why it was important that we find enough opportunity to streamline the business and do restructuring to compensate, or overcompensate actually, for the overhead infrastructure we need to build. So, it's reflected in the numbers. So, '16 includes an overhead structure that would allow Veritas to go public.

Matt Niknam: Can you quantify what that headwind is that hits in '16?

Thomas Seifert: It's actually not a lot, because you have to keep in mind that from a revenue perspective Veritas is going to be slightly north of $2.5 billion. So, in terms of how many treasury people you need, how many IR people you need, it's not a big part of cost that is going to be added.

Helyn Corcos: There's a question right here with Steve.

Steve Ashley: Thank you. Steve Ashley, Robert Baird. For the enterprise security business, you talked about in FY16 maybe growing that 1% to 6%, but in terms of the new products, are they more subscription based and are we going to see billings have a different growth kind of characteristic during that year than we might see in revenue? I'm not looking for exact numbers, just looking for some color around that.

Thomas Seifert: Do you want to …

Male Speaker: It's a combination of both. Services (inaudible) a lot more subscription focused. ATP is actually licensed with an option to do a subscription.

Thomas Seifert: So, we are not done on the pricing side for all of our products. So we are still exploring how we best monetize it. It's too early, other than the general trends that Balaji alluded to, to go into specifics, but we'll do this as we get closer to the launch.

Helyn Corcos: We have time for one more question. We have Walter right up front.

Walter Pritchard: Thanks for letting me in under the wire. So, two—actually, let me ask the question I care most about and then if there's time I'll ask a follow-up. You identified on that slide an $800 million annual opportunity around renewals, which, on the base of your revenues, is a pretty big number. The Company has been at renewals for a long time. Can you talk about where the low-hanging fruit still is in that opportunity there to get that 800?

Thomas Seifert: Most of the low-hanging fruits are covered, right, because, remember, getting our renewal program in shape was one of the big eight initiatives we drove. This is really take it to a next level and connecting the renewal process to the overall sales interaction and care part from a sales and customer experience perspective, and some additional things we things we think we have in flight to make sure that we, from a go-to-market perspective, really address the whole and have visibility across the whole spectrum of opportunities that are in front of us. So, today, we don't see all the—or if not 100% visibility, let's put it this way, and this is taking it to the next level. It would not be possible to get there without the ground work we have laid in fiscal year '15, but it's another significant driver of revenue.

Michael Brown: We already have the dedicated organization in place for renewals; we've talked about that previously, but we're incorporating more tools to be able to help that organization be more proactive to get renewals. So, example, we don't wait until 30 days before the renewal is due to start the process with those customers of checking to see how they feel about the value that they're receiving, and if they're not, what corrective action can we take. If you wait till the last 15 days before the renewal is coming due, it's already a done deal. If that customer were to call our support organization, we have connected the dots there to say, "Had a problem with support, this particular thing, how well was that solved?" We know that directly relates to how quickly and how enthusiastically they're going to renew. So, there's a lot more science that we're applying now to that renewal process than just having a sales person call on them 30 days before, and we're seeing improvements in the renewal rates as a result.

Walter Pritchard: Then just the second question I had is on fiscal '16, which understanding a lot of that is business you've booked this year, but as we look at '16, say, bookings into '17, with revenue—I mean, there could be a decent amount of kind of breakage in the business as you go through the separation, and I think a lot of us in the room here have the memory of before the sales force separation back in fiscal '14 early days, there was a lot of breakage around that, and so I guess on a lot of people's mind is how much have you embedded in the model for breakage in the business that could occur? Some, you can see risks you know and some are risks you may not know.

Thomas Seifert: I think the first point we're going to make is we look at what happened in the previous transaction and it was not so much—the first step was not about anticipating the breakage but preventing the breakage from happening, and this is why there was so much effort to enter the year with a separated sales force and not go through the separation during the fiscal year '16. We put our team in place, we put the coverage models in place, we put the sales incentives in place, we put the quotas in place, so we did all this work upfront so we don't have to touch the sales organizations anymore during the course of fiscal year '16. So, I think we have been rather diligent. We customized the whole separation timeline, the milestones, the work that needs that needs to be accomplished around that target. So it was really important from a resource and resource availability perspective that that part of the separation was covered, was covered upfront and early, and to great detail. Mike already applauded Brett and Adrian that they have been—and their teams have been able to do that. So a lot of work upfront and putting measures in place to make sure we have the right incentives in place to continue with the momentum that we have seen in fiscal year '15.

Michael Brown: Yes, the way we're thinking about it is it's not about breakage, it's about execution. We've outlined what I believe is a pretty compelling strategy. We've got the right talent in place. Now, it's about executing on that to deliver the growth.

Helyn Corcos: Great. So, that's the wrap on the Q&A. I think we're going to have just closing comments from Mike and then we'll finish up.

Michael Brown: So, you know, as I started the day, I started with my personal excitement about what I saw ahead for '16, and certainly continuing into '17, and I think what you've seen now from a number of presentations I hope gives you some sense of the confidence that we're feeling, both because the strategy has been very clear now—we worked very hard this past year on making sure that was clear for the organization—and the focus that we need to make sure that those strategies for our two businesses can lead us to more success going forward. So this is all about executing and achieving the growth. The focus, obviously, helped us expand our margins. We're taking that forward, as you saw in Thomas' presentation, as we look at '16 and '17 and we see opportunities to improve that over that timeframe.

We've also significantly changed our investments. So we've shifted not only R&D, but a lot of our go-to-market, to be focused on the higher growth areas. It takes a little more time to get the growth started and then to show through. You're seeing that to a big extent this year, as the tremendous number of new products come online both for Veritas and Symantec security, and of course even as they get introduced this year, we don't get a full year of their growth because they're introduced mid-way through the year. But one question I got during one of the breaks was how real is all of this? R&D is focused on this today. We're not talking about a vision that's 10 years out. We're talking about where our R&D resources are applied today. I'd encourage you to check out those demos because then you're going to see how real that is, and these products, these new products start to hit in Q1. So, we've got a very steady cadence of product introductions both on the Veritas side and Symantec security. That's part of what we mean when we say executing on our key operational priorities, those new products are key to us hitting the growth that we talked about. Those products, we think, leverage unique assets on both sides. Hopefully you saw that. On the Veritas side, we're taking that traditional heterogeneity, scale and strength of customer base to introduce brand new offerings that get availability and insight solutions that customers don't have today, they're very excited about.

Then on the security side, as you saw, the model for security is changing; it's all about what's my visibility, security analytics? No company in the industry is better positioned than Symantec to be able to take that scale that we offer and turn that into a customer benefit, so we're very focused on that. That's what Balaji and Amit and Jeff talked about a little bit earlier. So the combination of threat protection, information protection both on the unified security analytics platform and complemented by services; we know we've got the right offerings there to solve customer pain points. If we do that then what we show through for our shareholders who are in the audience as well as those of you who analyze the Company is growth, and I don't think it's any surprise that we believe that given the level of profitability we have already demonstrated, it's growth that's going to unlock the value for Symantec. So we very much look forward to reporting the year to you as it develops and to delivering on the things that we talked about here today.

Thank you very much for your attention through the day and I think now we're going to adjourn to both the demos and the reception—and Helyn, you have some logistics for us on that.

Helyn Corcos: I do. It's actually on the ninth floor, so we recommend that everyone take the far left elevator bank because that's the only that goes up to the ninth floor, and we will start at 2:00pm. Thank you very much.

Michael Brown: Thank you very much.