Enterprises face the challenges of an ever-changing set of risks. Literally every day there is a new vulnerability discovered, there's a new exploit to use that vulnerability, and there's a new tactic the attackers are trying to take. And that's not to scare an executive and focus really on the negative risks, but there's also the risks of just connecting with one another. And when I connect my environments to yours, we have shared risk and we have to understand the risk that that does pose to each of our organizations. And then, to top it off, we have changing technology. The rate of technology change is just really outpacing most organizations' ability to keep up with it. They want to move to cloud, their employees want to use mobile devices, and every day there's a new and different technology challenge that goes along with each of these security challenges. So, bringing that all together is just a really difficult mix, even for a seasoned IT executive. With all of the changing technologies and threats, organizations, be it a government, an industry group, are looking to provide guidance. They want to help us protect our banking data, they want to help us protect our energy and utilities and those infrastructures, they want to help us protect our credit card information as it goes through transactions. So, organizations look to standards such as the PCI DSS standard, they look to prescriptive guidance in the U.S., for example, from the FFIC on how to protect banking data, or they look broadly at global standards such as COBIT or the ISO 2700 series to just get some sense of what they should be doing. But not all of those line up really cleanly for one another,
so what executives need is they need
a very flexible framework that gives them
a frame of reference in
how they make decisions
and things to consider.
And then they can apply
the various standards
and regulations to that
and they'll make a lot more
sense as they come together.
The 10 essential practices
were put together
by our Chief Security Officer,
and it was her way to
talk to our other line
of business executives across IBM
about the risks and challenges of security
that they may be facing in
their individual business units.
Much like our customers face today
when they deploy their
own technology solutions
in their business.
So this was an easy framework of
10 key, essential practices
she could have with any
executive across the company
and be able to then
walk away with a better appreciation
of their risk tolerance, their
ability to manage that risk
and understand it.
The benefit of the IBM
10 essential practices is
that it's not prescriptive guidance.
It is a framework that
we want executives to use
when thinking about
security problems they face
when they're deploying new technologies
and solutions in support
of their business.