The key to identity and access management is understanding who you want to have access to your systems and data. And ensuring that they have a continued need for that access. When we talk with many companies today, we find that they have thousands of user accounts that are very difficult to manage. Often they have weak passwords. And then we find out that they don't re-validate those users on a regular basis which means they may have former employees that still have active accounts in their environment. All of this presents a really great risk to their systems. Because, as we talked in one of our earlier videos, trusted insiders are a great source of risk. Especially if they're not educated. But, if we don't go the extra step of making sure that the users have the access they need or when they no longer need it, such as when they're no longer working for us, then we can't get ahead of the hackers. We're gonna just make it very easy for them to walk in the front door, essentially. In a personal sense, who do we let into our homes? Do we let anyone off the street come into our home? Do we only let trusted friends or family come in through our front door? What about a cable repair man, perhaps, that comes knocking at your door saying he needs to come in to fix the cable because your neighbor's having trouble. Are you sure he's with the cable company? Does he really need to have access to your home? Or is he perhaps a thief who's looking to make his next heist? We really, through identity
and access management
want to know who's accessing
our home, our environment.
You know, in a technology sense.
And are they the right
group that we want to allow
to access and what should
they be accessing if they do
come into our homes or
into our IT environment?
Cloud and mobile really
complicate user ID and access
management.
Traditionally, we knew the
assets that were in our data
center environments, we
knew our users that were
accessing them.
But now as we have mobile
technologies we're doing more
social collaborations with
clients, with partners,
and our business applications
and data are moving
to the cloud, we really
go back to that problem of
everyone wants access to
everything from everywhere.
And that's a very difficult
problem to manage through
access control.
The good news is it is controllable,
but you have to take the time
and diligence to understand
who really needs to access
what data, what systems,
what applications, and
then manage it accordingly.
And do it on an ongoing basis.