In our personal lives, whether you realize it or not, many of us are using cloud today. If you have an iPhone, you are using probably iCloud. If you are using Gmail or Hotmail, your email is stored in a cloud. Even private information, such as when we go on vacation or maybe information about our personal financial position that we are sharing with our financial planner for example. That's all on the internet. It's stored in the cloud if you are using one of those cloud providers. What most people don't stop and think is what happens if a hacker were to gain access to that information. We like to think our email is private, but it's really not. The same goes for a business. When they put applications and data in a cloud, unless it's a private cloud, they are in a shared environment with shared risks of other cloud users and the IT provider that is giving them the cloud access. So they really need to think about the security controls both the cloud provider itself is using for the cloud infrastructure, but more importantly the controls that they as a cloud user need to have to protect their applications and data in that cloud. Only through working hand-in-hand with your cloud provider are you going to know that those controls are in place. You want to ask the cloud provider about the services and the technologies that you can employ within their environment to protect the data. Cloud offers many benefits to a business. It gives them more resiliency and availability of their systems. They can have more backup. It also offers the added benefit of being cheaper typically than deploying traditional IT infrastructure into a data center. But those benefits come with a risk as well. The risk is that typically organizations do not own the cloud environment. They are typically going to a third party provider. They have to work hand-in-hand and partner
with the cloud provider to ensure 
the right security controls are in place
not only to protect the 
cloud environment itself, 
but to protect the data and applications 
that the organization is placing within 
the cloud environment. 
Your move to cloud is one of the few times 
you are going to have 
a chance to start over 
with your security. 
You're considering the 
workload your moving 
to the cloud environment. 
Your considering the applications, 
the data that is going to be 
used in those applications. 
What is the right control 
for that application 
and that data given it's going to be in a 
shared or public cloud environment. 
That's very powerful, 
because having that opportunity to stop, 
think of the requirements, 
add them from the beginning, 
and build that environment 
with security in mind, 
that really brings true benefit, 
and it really increases 
your security posture 
compared to traditional IT environments.