Today, really, information is the new world currency. Just like money in banks has value, information today has substantial value. It's ultimately the whole reason why we have the security programs we do. It's interesting for a hacker to gain access to a system, or to a network, or through a network, but at the end of the day, the hackers, as I mentioned in one of the prior videos, earn a living, in many cases, by exploiting systems and gaining access to data. So, they wanna find that confidential data, the sensitive data, and this data has a street value. And an individual social security number can be worth roughly a dollar. Healthcare records can be worth 50 dollars or more each. Banking information, depending on the account balance in the bank and the type of banking information available, can go for over 1,000 dollars a record. And so, this really, when you think of the breaches you hear where tens of thousands or hundred thousand records or more were breached, this has real value to the cyber criminal out there today. And then, when you think about the added cost of the data breach, that is even more disconcerting and bring a bigger financial burden to an organization. In the 2015 Ponemon Cost of a Data Breach Study, we found that the cost per incident continues to rise. On average, it's about 3.8 million per incident, or roughly $154 per record, when a company experiences a data breach. The costs come from a variety of sources. It's not just the financial loss, perhaps, of that information, but it's everything from the cost to respond to that incident, to clean up that incident, install preventative controls, and then there are many intangible costs, such as the loss of customer loyalty. We've seen in some breaches, even there was a loss
of market cap by the companies when they had a breach. So, there are real financial and intangible, but still very relevant, losses, a company experiences when they have a data breach. At the end of the day, this is really one of the most critical areas of security is, thinking about the data that's involved. Within IBM, we advise our clients on a critical data protection program. We walk them through, starting with the data itself, and identifying what type of data is critical, or meaningful, what's important in generating their business and value in their organization. We start with that data and we work our way backwards. We classify the different systems and applications that may access that data, and that the other related data types that go with it. Then, we understand what controls do you need to put in place. Again, thinking from the inside out. How do you need to protect the applications that access that data? What are the users and the types of users? Who is using the data? Where does that data physically reside? What system does it sit on? And then, what are the network connections to those systems, and how do we need to protect those? Really, you think of it as a data-centric approach to security, rather than a network-centric approach, which has been what we have taken for more than the past decade.