Today, our businesses operate in a world full of risks on the internet. And everyone from the most senior executive down to the most junior employee needs to understand those risks. They need to know how to identify them, how to manage them, and how to mitigate or ideally, eliminate them. And so building a risk-aware culture is, in a sense, what we've done with our own personal health. We're aware of the diseases that are prevalent in the world. We wash our hands. We cover our cough or our sneeze. And we do things that try to prevent others from becoming sick, or from ourselves becoming sick. We want to have that same awareness in our employee base in an organization. We want them to just think about the internet risks and the security risks that are present as they do business on the internet. So the risks that we're talking about are the risk of unauthorized access, or the risk of data theft, data loss. In the news, every day, you hear about another organization having a security incident or a data breach. And it's not just that they've stolen the data. It's that they actually have a financial impact to that organization, or they may have an impact to the loss of their reputation and trust of their customers. So the technology is there to support the business. Security is an enabler to that technology so we can operate in a secure fashion. And we want to reduce the risks so that the businesses ultimately can become successful, and profitable, and maintain the trust and loyalty of their customers. And it's everything from having the right policies in place, the right practices so that they actually do the things that will help manage the risk, and a lot of education. Education is the most critical component to having a risk-aware culture.
When we have everyone take that education on at least an annual basis, but an ongoing basis, ideally, they can be better aware and understand the types of risks and the changing threat landscape that their business faces. And really, it's those employees who already have access to the systems and the data that often compose the greatest risk, not always intentionally, but sometimes through an inadvertent mistake they may click on email that has malicious code in it, just by accident because it looked interesting. And then their account's compromised. And again, it's them as the employee who really did allow that to happen, but through education, through being more aware, having that risk-aware mindset, often those types of inadvertent mistakes are easily prevented. Security is everyone's responsibility. Any user of technology in an organization has a responsibility to use it in a secure fashion.