Security is an integral part of developing any application. It needs to be considered throughout the earliest phases of the application concept, the business requirements and other functional requirements, through the development and ultimately deployment of that application in the environment. All too often, though, security is deprioritized, given the need to have speed to market or other development constraints to get the application ready. When we think of the software development lifecycle, we think of those requirements up front, but we also need to consider secure coding practices, and the security testing that should happen before any new release is rolled into production. Education for the developers is also key here. Again, it relates back to essential practice number one of a risk aware culture. You need to educate your developers on how they have to do secure coding and the importance of it, not only to the code, but ultimately to the use of the application. Consider it this way in the real world, would you build a museum housing priceless art and artifacts and not install the security controls or moisture controls or environmental controls that you need to protect that priceless art and artifacts? It's the same thing. This application is being built to run millions or billions of dollars of business for an organization, and it needs to also have the right security controls. Also, application security is not just for traditional business applications. Again, we've gotta think about our essential practice around mobile security. You must also have security in your mobile applications and devices that may be using that same application.
Would you trust your business to an application that has no security controls or that had not been tested? Unfortunately, many organizations do, and then they find out the impact of that after the fact, when they have a data breach.