Much like in our personal lives, an ounce of prevention is worth a pound of cure. We take care in our personal lives to wash our hands, to go to the doctor for preventative check-ups, and to do many things that keep us clean and healthy so that we have a longer life. We want to do the same thing with our IT assets and information. We need to put some very basic controls in place, such as patching our systems on a regular basis, adding the security patches when they come out, establishing security configuration standards and managing to those, or even installing some of the very basic and necessary security controls, such as anti-virus software on our endpoints. Through doing some of these very, very basic fundamental security actions, we really can prevent so many security incidents. We have good, secure configuration management, we have a resilient environment that has back-ups, data back-ups, network connectivity back-ups, that we're patching. I can't stress the importance of patching, both from an application functionality standpoint and a security standpoint because that is going to take care of so many potential avenues for exploit by just doing some of those very simple, basic, really fundamental security actions or IT management actions that can prevent those incidents. I can't tell you the number of incidents that I have personally worked where the vulnerability was several years old. The organization had plenty of time to patch and to fix that vulnerability, yet they chose not to and they were subsequently exploited and lost data and money because of it.