MISCONFIGURED CAMERA LEAVES TECH COO'S HOME EXPOSED FOR OVER 3 YEARS

The Chief Operating Officer ("COO") for a large U.S. technology company hired BlackCloak to protect the high-profile family from cyberthreats. The client had the highest-grade security cameras professionally installed years earlier to monitor the house, the children and home personnel, and she was now seeking BlackCloak to round out her sphere of cyber protection.

During its vulnerability scanning of the entire home, BlackCloak identified that the existing security controls on the security cameras were not enabled and other settings misconfigured. The cameras were in turn sending unencrypted feeds across the internet and all of the cameras were accessible to anyone on the internet. All an attacker had to do was use scanning technologies to locate the publicly facing cameras and use the default credentials that had not been changed to peer into the private life and home of the client.

Obviously, this powerful security tool for someone with physical security risks was potentially turned into a weakness and potentially tool for spying on the family and their children.

BlackCloak provided the client and their provider with the steps necessary to harden the security settings on f the cameras (thus closing off the camera access to the Internet) and successfully secured the home.