Critical Infrastructure Intrusion

Russell Smith
Australian Institute of Criminology

Perhaps the most critical step in the commission of a cybercrime is gaining access to a computer network in such a way that one's identity will not be revealed to law enforcement and regulatory authorities. In the early years of computing, little attention was given to identifying users, with minimal logon protocols being used and poor verification checks undertaken of the often rudimentary evidence of identity submitted. As cybercrime developed in scale and impact, and as criminal justice responses began to take on new levels of importance, the necessity to regulate user authentication became essential and we now have a plethora of policies and procedures aimed at identifying individual users with assurance. This paper explores the ways in which cybercriminals have responded to cyber security measures used to authenticate identity and the crime displacement effects that have been created as a result. The future will see user authentication crime adapting in response to new biometric technologies that, while enhancing our ability to authenticate identities with certainty, may lead to a variety of counterproductive consequences.