



## Colaborative Security

Denise Anderson

Traditionally healthcare IT has been focused on privacy and data protection particularly under the lens of HIPAA violations. However incidents like the May 12th 2017 global WannaCry campaign and the June 27th 2017 Petya (NotPetya) campaign demonstrate that healthcare delivery organizations cannot ignore the disruption, financial and reputation impacts of cyber attacks. This session will discuss how information sharing and collaboration amongst healthcare and other critical infrastructure stakeholders can help entities use one organization's defense for their offense as well as extend their cybersecurity protective measures. It will cover the threat landscape for healthcare and particularly look at threat actors, motivations and tactics, techniques and procedures (TTPs) used for attack. The session will look at specific case studies such as mitigation strategies and other information shared during WannaCry, Petya and other incidents. Learning Objectives: Participants attending this session will learn; • The threat landscape in healthcare and threat actor motivations and techniques • Why cybersecurity needs to become a Boardroom issue. • The impacts of cyber attacks on organizations The role of information sharing in community defense and • Strategies for affordable means to protect against cyber attacks.