Cyber Threats in Healthcare: how organisational culture affects hospitals' cyber resilience

Marselia Tan
Department of Health Policy

Modern technology has brought unprecedented improvement in speed and efficiency to health systems, while also increases its susceptibility to cyber-attacks. Still fresh in memory is the WannaCry attack affecting more than 40 NHS organisations –risking patients' safety, disrupting services, and creating huge financial damage. Crucially, healthcare is the only sector in which sources of threats are more often internally driven rather than from outside, with employee's abuse or misuse or data as well as human errors contributing to the increased risk. This implies a systematic weakness in the organisational culture in which employees of health systems work.

As the direct consequence of cyber-attacks in health systems can have immediate harm on people's lives, it is important to identify what makes this industry particularly vulnerable internally in order to formulate proper policy responses. Qualitative interviews with clinical and supporting staff from hospitals across various sizes and specialties are planned. The study aims to understand health employees' perceptions about their professional responsibilities, personal values, sense of loyalty to the employer organisation, and management style and attitude toward technology within their places of work. These insights are expected to reflect the hospitals' existing organisational cultures and the potential areas of internally-driven vulnerabilities in the context of protection of sensitive medical data.