|  |
| --- |
| ***SANL*** |
| **STRENGTHS (+)** | **WEAKNESSES (-)** |
| * Realistic training
* Training material tailored to the healthcare domain
* Adaptable training to track changes in organizational needs & changes in the threat landscape
* Support for the establishment of fine-grained & dynamic CSLAs
 | * Infrastructure requirements for cyber range environment
* Setup & maintenance needs (technical challenges, personnel needs)
* Complexity of definition of new training programmes
* No previous experience or integration into business processes of continuous training
*
 |
| **OPPORTUNITIES (+)** | **THREATS (-)** |
| * Coarse, not organization-specific, nor dynamic (C)SLA establishment typically within healthcare sector
* Lack of awareness of cybersecurity training benefits & cost-effectiveness
* Significant barriers to adoption of cyber range training within healthcare organisations
* Lack of a shared knowledge base of training programmes shareable across organisations
 | * Resistance from 3rd party providers to adopt CSLAs
* Resistance from higher management to provide the resources needed (cost, personnel) to establish and maintain cyber range environment
*
 |