Gestion des risques: Cyberattaques, stress hospitalier

ID: 39

Cyberattaque au Centre hospitalier Sud Francilien: Ressenti des personnels d'anesthésie médecine péri opératoire (AMPO) et du bloc opératoire

E. Brocas*(1), A.Carriol(2), A.Batista(2)

(1) ANESTHESIE MEDECINE PERI OPERATOIRE, CENTRE HOSPITALIER SUD FRANCILIEN, Corbeil essonnes, France , (2) DQGR, CENTRE HOSPITALIER SUD FRANCILIEN, Corbeil essonnes, France

**Auteur présenté comme orateur*

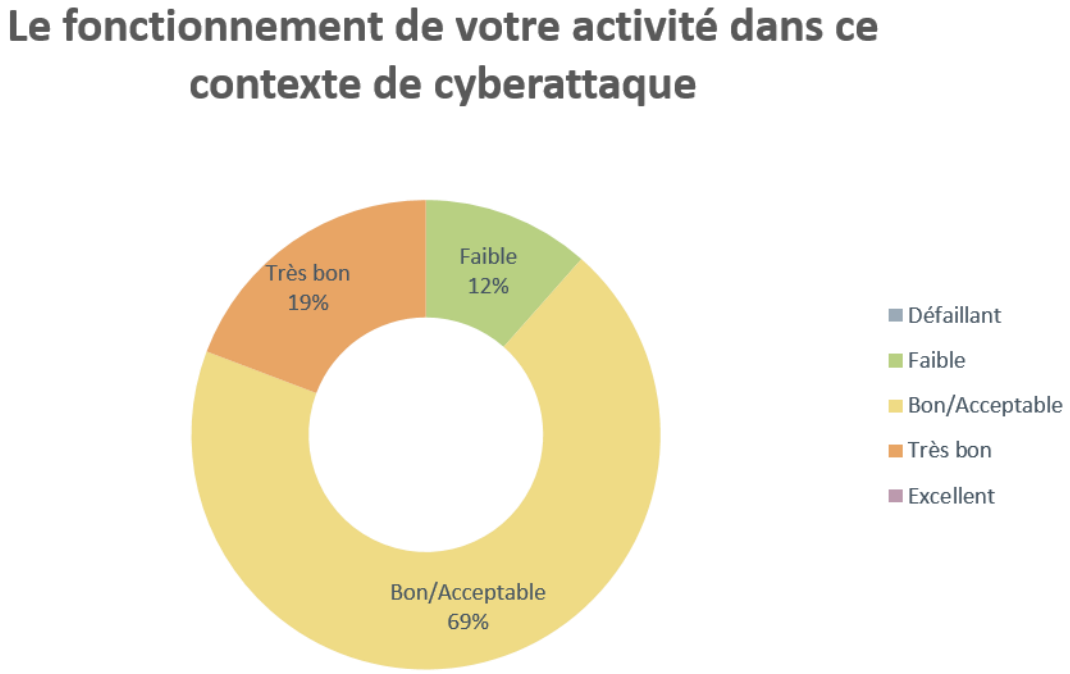
Position du problème et objectif(s) de l'étude:
Depuis plusieurs d'années, le cyberterrorisme s'est déployé massivement, attaquant notamment les établissements de santé. Le 21 août 2022, notre établissement a été attaqué par un rançongiciel bloquant presque toute la totalité du système d'information. Le service d'AMPO et le bloc ont du se réorganiser en urgence pour continuer d'assurer la prise en charge des patients.
Nous présentons le ressenti des personnels (médecins, paramédicaux, secrétaires...) face à cette situation critique inédite.

Matériel et méthodes:
Enquête menée en partenariat avec la cellule gestion des risques en décembre 2022 via 2 modalités :
1) Entretiens semi directifs auprès des personnes "clefs": chef de bloc, cheffe de service anesthésie, MAR référente obstétrique, MAR référent ambulatoire, régulateur bloc, secrétaire de bloc, secrétaires d'anesthésie, cadres.
Thèmes: le vécu de l'attaque, les premières mesures prises, les étapes du retour à la normale, le bilan et enseignements à retirer de cette expérience.
Pour chaque thème, les actions et objectifs, les facteurs de réussite, les difficultés et les enseignements ont été notés
2) Questionnaires semi-directifs auprès de l'ensemble des personnels: thèmes abordés: l'alerte, organisation et mesures prises, impacts personnel et professionnel, les changements d'habitude en terme de cybersécurité, l'évaluation globale de l'adaptation à la crise.
Les résultats sont présentés sous forme de statistiques descriptives

Résultats & Discussion:
1) Entretiens: Est rapporté le souci premier de sécuriser la prise en charge patient et de trouver des outils permettant un maintien de l'activité (programme opératoire, agenda de consultation). C'est passé par une communication accrue, anticipation et adaptabilité constantes et une centralisation des décisions autour de personnes ressources (chef de bloc, cheffe de service AMPO, secrétaires).
Un nuage de mots décrivant l'expérience a été généré (fig.1).
2) Questionnaires(n= 26): apprenant l'attaque, seuls 50% en ont perçu l'impact (25% des médecins). Le plus critique fut l'absence de biologie/imagerie/dossier, la perte du serveur de stockage et celle des programmes opératoires et de consultation.
En termes d'impact personnel, les personnels sont rapporté la perte de documents et la peur que leurs données personnelles soient utilisées de façon malveillante.
La sécurité des soins a été jugée priorisée à 88%.
La réponse à la crise est majoritairement jugée acceptable à très bonne (fig.2).

Conclusion:
La cyberattaque dont notre établissement a été victime a fortement impacté le quotidien des soignants du bloc opératoire et du service d'anesthésie.
Les mots clés témoignant des soucis premiers des personnels ont été: pilotage, organisation, sécurité

des soins, vigilance et adaptabilité. L'identitovigilance a été perçue comme un point critique crucial; de même que la maternité a été identifiée comme un secteur particulièrement vulnérable (en raison du risque hémorragique).
La crainte de perte et/ou d'utilisation malveillante des données personnelles a été également au premier plan.
Cependant, face à la crise engendrée par la cyberattaque, les personnels du service d'anesthésie et du bloc opératoire se sont rapidement adaptés et sont globalement satisfaits du maintien de la qualité de prise en charge des patients.



Les auteurs déclarent ne pas avoir toute relation financière impliquant l'auteur ou ses proches (salaires, honoraires, soutien financier éducationnel) et susceptible d'affecter l'impartialité de la présentation.