Mélina CHASTANG GIUNCHI

Entre pression technologique et souffrance mentale : étude des impacts psychologiques des cyberattaques sur les RSSI en milieu hospitalier

Université BORDEAUX MONTAIGNE
Cyber criminalités

Promotion 2024-2025

Introduction

Depuis l'essor massif des technologies numériques, notre société a basculé dans une ère d'hyperconnexion. Chaque acte de la vie quotidienne - consulter un médecin, inscrire un enfant à l'école, faire ses démarches administratives - implique désormais la transmission d'informations sensibles via Internet. Cette transformation a apporté des avantages notables : rapidité des échanges, simplification des procédures, accès élargi à l'information. Cependant, cette numérisation généralisée a aussi son revers : l'exposition croissante des données personnelles aux cybermenaces.

Le secteur de la santé, en particulier, est devenu une cible privilégiée des cybercriminels. Les hôpitaux français ont été à plusieurs reprises la proie de cyberattaques massives, paralysant leurs systèmes informatiques et compromettant la prise en charge des patients. Ces attaques ne sont pas sans conséquences humaines : elles exercent une pression intense sur les professionnels chargés de protéger ces infrastructures critiques, notamment les Responsables de la Sécurité des Systèmes d'Information (RSSI). Ceux-ci se retrouvent en première ligne, confrontés à des crises techniques et éthiques majeures, dans un climat d'urgence permanente.

Face à cette réalité, une question centrale émerge :

Dans quelle mesure les cyberattaques ciblant les établissements de santé affectent-elles la santé mentale des professionnels de la cybersécurité, et comment des biais cognitifs tels que la normalisation du risque ou la réticence à exprimer la souffrance psychologique influencent-ils cette perception ?

Afin d'explorer cette problématique, cette recherche s'appuie sur une double approche : l'analyse quantitative d'un questionnaire évaluant les symptômes de stress, d'anxiété, de dépression et de TSPT chez des RSSI, ainsi qu'une série d'entretiens cliniques permettant d'approfondir leur vécu subjectif.

Trois hypothèses structurent cette enquête :

1. Les cyberattaques dans les établissements de santé génèrent un stress psychologique important chez les RSSI, qui se manifeste par des symptômes de TSPT, d'anxiété et de dépression.
2. Certains facteurs contextuels (ancienneté, soutien, formation, répétition des exercices) semblent moduler l'intensité de la souffrance psychologique, en favorisant des mécanismes de résilience.
3. Des biais cognitifs (normalisation du stress, inhibition émotionnelle, stigmatisation) contribuent à la sous-estimation ou au déni de cette souffrance, limitant la demande d'aide ou la reconnaissance institutionnelle du phénomène.

À travers cette étude, il s'agira donc de mieux comprendre l'impact psychologique réel des cyberattaques sur les professionnels de la cybersécurité hospitalière, et d'interroger les mécanismes de défense, de résilience et de vulnérabilité propres à ce champ encore peu exploré.

Études académiques et recherches sur le stress chez les professionnels de la cybersécurité.

Il y a peu de sources, mais cela reste significatif avec:

1. **U**ne étude publiée dans le *Journal of Global Security Studies* indique que les cyberattaques peuvent provoquer des niveaux de détresse psychologique comparables à ceux causés par le terrorisme conventionnel .
2. Un article intitulé "It's Time to Break the SOC Analyst Burnout Cycle" discute des causes du burnout parmi les analystes SOC et propose des solutions pour y remédier .
3. **U**n article intitulé "The Devastating Business Impacts of a Cyber Breach" publié en mai 2023 discute des risques croissants en matière de cybersécurité et de leurs impacts potentiels .
4. **L**a revue *Cyberpsychology, Behavior, and Social Networking*.
5. **Livres sur le stress et la cybersécurité**
    - "*Cybersecurity and Cyberwar: What Everyone Needs to Know*" par P.W. Singer & Allan Friedman
      Il fait une vue d'ensemble des enjeux de la cybersécurité, y compris les pressions psychologiques exercées sur les experts en sécurité.
6. **Articles et rapports spécialisés**
    - 1. Un article intitulé "Managing the emotional toll cybersecurity incidents can take on your team" publié par CSO Online en mars 2025 aborde les défis mentaux auxquels sont confrontés les professionnels de la cybersécurité .
    - 2. Un article intitulé "Persistent Burnout Is Still a Crisis in Cybersecurity" publié par Dark Reading en mai 2024 discute du problème persistant du burnout parmi les professionnels de la sécurité .

Ces ressources Etrangères soulignent les défis mentaux et le stress auxquels ces professionnels sont confrontés, ainsi que l'importance de mettre en place des mesures pour prévenir le burnout et promouvoir le bien-être mental.

Des études menées en France mettent en évidence les impacts psychologiques des cyberattaques sur les professionnels de la cybersécurité.
Selon un rapport publié en octobre 2024 par SoSafe, 56 % des professionnels français de la cybersécurité souffrent d'épuisement professionnel, dont 24 % présentent un risque élevé de burnout.[1]

[1] https://maker-system.com/actualites/epuisement-professionnel-cybersecurite-france-2024/

La problématique que cela soulève et comment y répondre?

Selon un article du *Monde* publié le 4 novembre 2024, environ 15 000 professionnels manquent dans le domaine de la cybersécurité en France, alors que le secteur compte actuellement entre 30 000 et 35 000 professionnels en poste. Cette pénurie, combinée à une diversification rapide des compétences requises, peut entraîner une charge de travail accrue et un stress significatif pour les techniciens en place.

En résumé, bien qu'il n'existe pas, à notre connaissance, d'études françaises spécifiques sur le TSPT chez les techniciens en cybersécurité, les conditions de travail dans ce secteur suggèrent une exposition potentielle à des niveaux élevés de stress. Des recherches supplémentaires seraient nécessaires pour évaluer précisément l'impact de ces facteurs sur la santé mentale de ces professionnels en France.

La première cyberattaque majeure recensée dans un hôpital français remonte à mars 2019, lorsque le Centre Hospitalier Universitaire (CHU) de Montpellier a été victime d'une attaque par hameçonnage (phishing). Un employé a ouvert un e-mail malveillant contenant un virus, ce qui a entraîné l'infection de plus de 600 ordinateurs. Heureusement, grâce à l'utilisation de réseaux internes indépendants, la propagation du virus a été limitée, évitant ainsi une contamination totale du parc informatique de l'établissement. [2]

Depuis cet incident, les cyberattaques contre les établissements de santé en France se sont multipliées, ciblant notamment des hôpitaux tels que le Centre Hospitalier Sud Francilien en août 2022 et l'hôpital André-Mignot à Versailles en décembre 2022. [3]

Avril 1998 : Une clinique parisienne est victime d'une cyberattaque, entraînant la mort de deux patients. [4]

Nice, Avril 2024 : Le Centre Hospitalier Simone Veil de Cannes, situé près de Nice, a subi une cyberattaque majeure le 17 avril 2024. L'incident a entraîné l'annulation de nombreuses opérations chirurgicales non urgentes et le report de consultations. Une cellule de crise a été activée pour gérer la situation, et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été sollicitée pour accompagner l'établissement dans la gestion de l'incident. [5]

L'**ANSSI** [6](**Agence nationale de la sécurité des systèmes d'information**) a été créée le **7 juillet 2009**.

2 stormshield.com
3 netexplorer.fr+1Wikipédia+1
4 ina.fr
5 Le Figaro+1securityaffairs.com+1
6 www.ssi.gouv.fr

Elle a remplacé la **Direction centrale de la sécurité des systèmes d'information (DCSSI)**, qui existait depuis **2001**. Cette transformation a marqué une volonté du gouvernement français de renforcer la cybersécurité nationale face à l'augmentation des menaces numériques.

Depuis sa création, l'ANSSI joue un rôle central dans la protection des infrastructures critiques et accompagne les entreprises et les administrations dans la sécurisation de leurs systèmes d'information.

Missions de l'ANSSI

- **Protéger** les infrastructures critiques françaises (hôpitaux, administrations, entreprises stratégiques, etc.) contre les cyberattaques.
- **Aider** les organisations à renforcer leur sécurité informatique et à réagir en cas d'incident.
- **Surveiller** et analyser les menaces cyber pour anticiper les attaques.
- **Sensibiliser** et former les acteurs publics et privés aux bonnes pratiques de cybersécurité.

Exemples d'actions de l'ANSSI

- Intervention après des cyberattaques majeures, comme celles ayant touché des hôpitaux.
- Certification de solutions de cybersécurité utilisées par l'État et les entreprises.
- Publication de guides et de recommandations pour améliorer la sécurité des systèmes d'information

Méthodologie dans cette approche

Le Questionnaire

Cette étude porte sur les structures hospitalières publiques. Depuis quelques années, ces établissements font face à des cyberattaques qui pénalisent leur fonctionnement pendant des périodes variables. Lors de ces incidents, des équipes techniques se mobilisent pour soutenir la structure et son personnel, tandis que les patients en subissent directement les conséquences. Le personnel, quant à lui, se mobilise et recherche activement des ressources pour faire face à ces situations critiques.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) doit faire preuve de réactivité et proposer rapidement des solutions techniques pour restaurer la sécurité de la structure. Cependant, derrière ces procédures et prouesses techniques, se posent des questions importantes quant à l'impact psychologique sur les professionnels impliqués, et notamment sur les conséquences à moyen et long terme.

Afin d'approfondir cette problématique, j'ai conçu un questionnaire visant à explorer ces pistes. Mon hypothèse principale est que ces interventions pourraient être associées à des symptômes de Trouble

de Stress Post-Traumatique (TSPT). Avec l'aide d'un professionnel du secteur, il est envisagé de solliciter 90 personnes travaillant dans ce contexte, principalement au sein du service RSSI.

Les participants recevront un mail de présentation accompagné d'une invitation à un entretien clinique. Un questionnaire leur sera également adressé pour mettre en évidence, grâce à un diagnostic différentiel basé sur le DSM-5, d'éventuels symptômes associés.

Pour éviter les biais cognitifs, les questions ne sont pas présentées dans un ordre préétabli. L'ensemble des retours permettra d'orienter la réflexion.

Conception du Questionnaire

Le questionnaire se structure autour de 4 axes de réflexion :

- **Section 1 : Symptômes du Trouble de Stress Post-Traumatique (TSPT)**
- **Section 2 : Symptômes Dépressifs**
- **Section 3 : Symptômes Anxieux**
- **Section 4 : Autres Symptômes Psychologiques**

Pour chaque section (non visible par la cible), une série d'affirmations est proposée, évaluées sur une échelle de perception :

- **0 : Pas du tout**
- **1 : Un peu**
- **2 : Modérément**
- **3 : Beaucoup**
- **4 : Extrêmement**

Interprétation des Scores

- **Section TSPT** : Score total sur 7 items (maximum 28)
- **Section Dépression** : Score total sur 7 items (maximum 28)
- **Section Anxiété** : Score total sur 6 items (maximum 24)
- **Section Autres Symptômes** : Score total sur 4 items (maximum 16)

Une interprétation indicative suggère qu'un score élevé dans une section peut indiquer la présence de symptômes importants dans ce domaine. Aucun seuil défini n'est fixé ici, l'interprétation devant être réalisée par un professionnel, qui prendra en compte l'ensemble du contexte de la personne.

Lecture des résultats obtenus (données, observations, analyses, etc.)

1. Prévalence des Symptômes et Scores Globaux

- **Trouble de Stress Post-Traumatique (TSPT) :**
  Les scores dans la section TSPT indiquent que bon nombre de professionnels ressentent des symptômes significatifs. Une moyenne élevée sur les 7 items (sur un maximum de 28) suggère que la gestion des incidents de cybersécurité dans des environnements critiques, comme les établissements hospitaliers, représente une source de stress intense.

- **Symptômes Dépressifs et Anxiété :**
  Les scores des sections dédiées à la dépression (7 items, max 28) et à l'anxiété (6 items, max 24) montrent également des niveaux modérés à élevés. Cela laisse penser que le stress lié aux cyberattaques ne se limite pas au TSPT mais s'accompagne d'un impact global sur l'humeur et l'état anxieux des RSSI.

- **Autres Symptômes Psychologiques :**
  La présence d'autres symptômes, évaluée sur 4 items (max 16), vient compléter le tableau en soulignant des répercussions possiblement moins spécifiques mais tout aussi perturbatrices sur la santé mentale des intervenants.

2. Variabilité des Réponses

- **Hétérogénéité des Scores :**
  L'analyse des réponses montre une variabilité importante d'un individu à l'autre. Certains RSSI présentent des scores relativement faibles, peut-être en raison d'une expérience ou d'un soutien institutionnel fort, tandis que d'autres affichent des scores élevés, témoignant d'une vulnérabilité plus marquée face aux situations de crise.

- **Influence de l'Expérience et des Conditions de Travail :**
  Les données suggèrent que des facteurs tels que l'ancienneté dans le poste, le niveau de formation en gestion du stress ou encore la qualité des ressources disponibles lors des incidents jouent un rôle modérateur dans l'impact psychologique.

3. Implications pour la Santé Mentale et Recommandations

- **Charge Psychologique Importante :**
  L'ensemble des scores indique que les professionnels de la cybersécurité dans le secteur hospitalier font face à une charge psychologique non négligeable. Les chiffres témoignent d'un environnement de travail potentiellement propice au développement de troubles liés au stress, y compris le TSPT.

- **Nécessité d'Interventions Préventives et de Soutien :**
  Ces résultats renforcent l'idée qu'il est indispensable d'envisager des dispositifs

d'accompagnement, tels que des formations à la gestion du stress, des séances de débriefing systématiques après incidents, ainsi que l'accès à un soutien psychologique spécialisé.

- **Pistes pour des Études Futures :**
  Le sondage ouvre la voie à une exploration plus approfondie, notamment pour déterminer des seuils de scores pouvant être utilisés comme indicateurs précoces d'un risque accru de TSPT ou d'autres troubles. Une approche longitudinale pourrait permettre de suivre l'évolution de ces symptômes et d'évaluer l'efficacité des mesures de soutien mises en place.

<u>Le faible nombre de retours et d'entretiens cliniques peut en effet conduire à plusieurs réflexions et hypothèses :</u>

1. **Réticence à Se Dévoiler :**
   Il est possible que les professionnels hésitent à partager des aspects intimes de leur vécu émotionnel, en raison de la stigmatisation associée aux troubles psychologiques ou par crainte de remettre en question leur expertise et leur capacité à gérer le stress inhérent à leur métier.

2. **Normalisation du Stress :**
   Le fait que le stress soit constamment présent dans ce secteur peut conduire à une forme de résilience ou de déni. Les professionnels pourraient percevoir leur vécu comme une partie normale de leur quotidien, et donc ne pas considérer la nécessité d'en parler ou de chercher un soutien psychologique.

3. **Biais de Sélection :**
   Ceux qui acceptent de participer aux entretiens pourraient être les moins affectés ou, au contraire, les plus en souffrance, créant ainsi une distorsion dans la représentation globale de l'impact psychologique. Ce biais de participation peut limiter la représentativité des résultats et influencer l'interprétation de la prévalence des symptômes.

Ces éléments invitent à approfondir la démarche en cherchant à comprendre non seulement l'impact des événements sur la santé mentale, mais aussi les facteurs psychosociaux qui influencent la volonté ou la capacité des professionnels à s'exprimer sur leurs expériences.

Synthèse des Entretiens Cliniques

Les entretiens cliniques réalisés avec les professionnels apportent une dimension qualitative riche aux résultats du questionnaire.

1. Parcours et Expériences Marquantes

- **Le premier** retrace son parcours débutant en 2020, marqué par une première reconnaissance lors d'une intervention suite à une attaque. Il évoque la transformation de cet événement en un tremplin professionnel. Cependant, il décrit ensuite des épisodes de stress extrême lors de crises, notamment lors d'une attaque simultanée qui a impacté un bloc opératoire, générant un sentiment d'impuissance et une culpabilité intense.

- **Le second** distingue deux types de stress :
    - Un stress permanent lié à la surveillance quotidienne et aux sollicitations internes, hypervigilance.
    - Un stress aigu lors des alertes, avec des conséquences sur son sommeil et une alternance entre pessimisme et dynamisme, trouble psychosomatique.
- **Le troisième** ayant vécu deux cyberattaques majeures dans un centre hospitalier, met en lumière la profondeur de l'impact psychologique que peuvent provoquer ces événements. Son témoignage fait écho aux symptômes identifiés dans l'étude, mais va plus loin encore, en illustrant la dimension traumatique, sociale et existentielle de la crise cyber. Il nommera la sensation d'un « entant numérique ».
- **Le dernier** met en lumière la fatigue due aux sollicitations continues et critique le manque de vigilance du personnel. Il évoque une normalisation du risque qui, malgré des exercices réguliers, ne dissipe pas complètement le stress et la pression ressentis.

2. Aspects Psychologiques et Résilience

- **Hypervigilance chronique et Épuisement :**
  Les témoignages soulignent une hypervigilance permanente, avec des pics d'intensité extrême lors des attaques (stress aigu, quasi-effondrement, insomnies) qui se traduisent par une fatigue physique et mentale importante.
- Elles génèrent **des micro-traumatismes répétés** et un **effondrement identitaire**. Le témoignage met en évidence un **clivage douloureux entre les techniciens et les autres services** : les premiers sont vus comme responsables (des coupures…), incompris dans leur rôle de protection. Les techniciens sont stigmatisés, parfois même méprisés, face à des médecins valorisés par leur mission vitale. Le plus alarmant reste l'**effet différé du traumatisme** : perte de confiance, syndrome de l'imposteur, burnout, voire suicides. On parle d'un sentiment de **culpabilité ingérable.**
- **Dilemmes Éthiques et Sentiment d'Isolement :**
  Les RSSI se trouvent confrontés à des décisions lourdes de conséquences (par exemple, couper Internet pour stopper l'attaque) qui engendrent une culpabilité anticipée et un isolement, parfois exacerbé par un manque de communication des autorités ou des collègues.
- **Perception du Risque et Normalisation :**
  Malgré la répétition des crises, une forme de mécanisme d'habituation apparaît, où les professionnels apprennent à relativiser les risques. Toutefois, cette normalisation ne suffit pas à atténuer le stress chronique accumulé, laissant transparaître des symptômes évocateurs d'un TSPT.

Parallèle entre Données Quantitatives et Entretiens Cliniques

1. Convergence des Résultats

- **Charge Psychologique Importante :**
  Tant le questionnaire que les entretiens révèlent une charge mentale élevée. Les scores quantitatifs indiquent des niveaux significatifs de TSPT, dépression et anxiété, ce qui est confirmé par les témoignages détaillés des RSSI, qui évoquent des états de stress extrême et des difficultés à se détacher émotionnellement des crises.

- **Impact des Situations de Crise :**
  Les épisodes de crise décrits lors des entretiens (ex : attaque sur le bloc opératoire, exfiltration de données massives) illustrent concrètement les situations qui génèrent les pics de stress quantifiés par le questionnaire. La réactivité exigée et l'incertitude constante apparaissent comme des facteurs déclencheurs majeurs.

2 .Divergences et Nuances

- **Résilience et Adaptation :**
  Certains témoignages mentionnent une capacité à "rangé ses souvenirs" ou à trouver dans la répétition des exercices une forme d'habituation. Ces aspects, moins apparents dans les scores bruts du questionnaire, suggèrent l'existence de mécanismes de coping et de résilience individuels et collectifs.

- **Manque de Détails sur les Séquelles à Long Terme :**
  Bien que le questionnaire permette d'identifier des symptômes, les entretiens révèlent que les professionnels ne partagent pas toujours en détail leurs ressentis ou séquelles, parfois par crainte ou par volonté de minimiser l'impact perçu, ce qui complique une analyse approfondie des conséquences à moyen et long terme.

Recommandations et Perspectives

- **Mise en Place de Cellules de Soutien :**
  Il apparaît essentiel d'instaurer des dispositifs de soutien psychologique pour les RSSI, avec des séances de débriefing systématiques après chaque incident majeur.

- **Formation et Sensibilisation :**
  Proposer des formations régulières à la gestion du stress et à la résilience pourrait aider à mieux préparer les équipes à faire face aux crises. L'analyse de la pratique professionnelle serait un outils idéal.

- **Optimisation des Procédures de Crise :**
  La révision des protocoles de gestion de crise, incluant une communication transparente avec le personnel médical et les autorités, est cruciale pour réduire la charge psychologique sur les RSSI.

- **Allocation de Ressources Adéquates :**
  Un investissement accru dans les ressources humaines et techniques (par exemple, renforcement des équipes, outils d'intelligence artificielle améliorés) pourrait atténuer les conséquences psychologiques des cyberattaques.

- Un **besoin de cellules psychologiques similaires à celles déployées après un attentat**, car selon eux, **« une cyberattaque est un attentat numérique. »**Créer des dispositifs de soutien psychologique pérennes. Reconnaître officiellement les cyberattaques comme des événements à **fort potentiel traumatique**, au même titre que les attentats ou les catastrophes naturelles.
- Revaloriser le rôle du technicien en crise.
- Mis en place de **Analyse de la pratique professionnelle au quotidien.** (APP)

Conclusion

Les résultats issus du questionnaire et les témoignages cliniques convergent pour confirmer que les cyberattaques dans les établissements de santé génèrent effectivement un stress psychologique significatif chez les RSSI. Cette pression intense se manifeste par des symptômes de TSPT, d'anxiété et de dépression, ce qui valide la première hypothèse. La gravité de cette souffrance souligne l'urgence à renforcer les dispositifs d'accompagnement psychologique et à améliorer les conditions de travail, notamment par la mise en place de cellules de soutien et une meilleure gestion des ressources, afin de favoriser la résilience de ces professionnels.

Concernant la deuxième hypothèse, l'analyse révèle que certains facteurs contextuels, tels que l'ancienneté, le soutien institutionnel, la formation spécifique, ainsi que la répétition des exercices de simulation, RETEX et exercices de mis en situation semblent moduler l'impact psychologique. Ces éléments peuvent agir comme des mécanismes de résilience, atténuant la gravité des symptômes et aidant à mieux gérer le stress lié aux cyberattaques. Cependant, ces facteurs doivent être explorés plus en profondeur pour confirmer leur rôle protecteur et orienter des stratégies d'intervention adaptées.

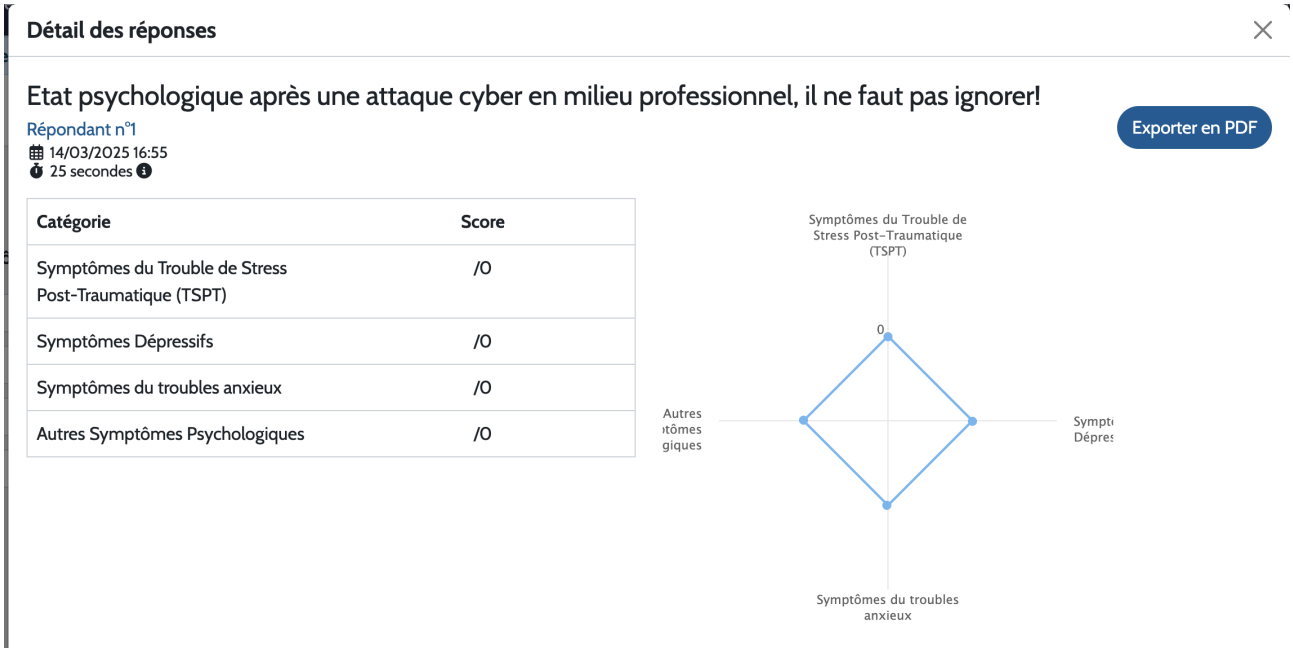
Enfin, la troisième hypothèse est également corroborée par nos observations. Des biais cognitifs, notamment la normalisation du stress, l'inhibition émotionnelle et la stigmatisation autour de la santé mentale, contribuent à une sous-estimation ou au déni de la souffrance psychologique chez ces professionnels. Cette situation limite leur demande d'aide et freine la reconnaissance institutionnelle du phénomène, ce qui complique la mise en place de mesures adaptées. Il apparaît ainsi nécessaire de sensibiliser et de déstigmatiser ces problématiques pour encourager une démarche de soutien plus ouverte et efficace.

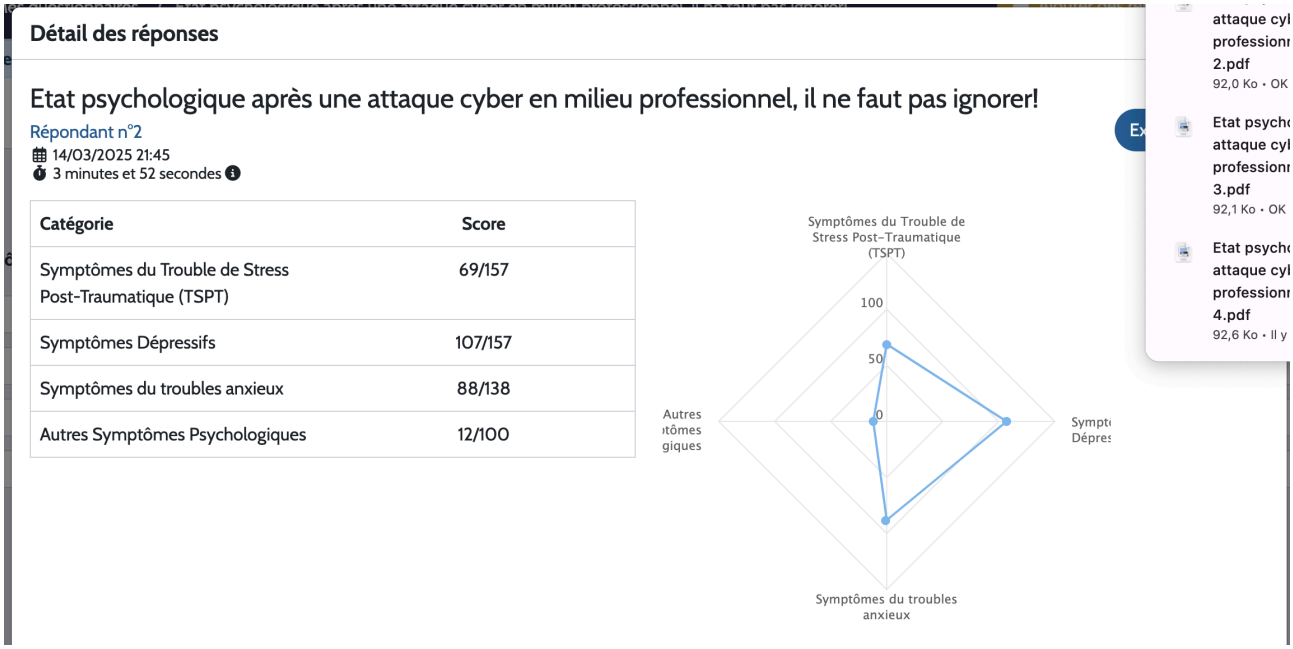
En résumé, cette étude confirme que les cyberattaques provoquent un stress psychologique majeur chez les RSSI en milieu hospitalier, modulé par certains facteurs contextuels et entravé par des biais cognitifs. Elle souligne l'importance de développer des stratégies d'accompagnement globalisées, incluant la prévention, la formation, et la lutte contre la stigmatisation, afin de mieux soutenir ces professionnels face aux cybermenaces futures. Des études longitudinales et approfondies sont nécessaires pour suivre l'évolution des symptômes, évaluer l'efficacité des mesures en place, et identifier des facteurs de résilience plus précis.

Le rôle des techniciens de l'ombre, est souvent indispensable mais il faut garder en mémoire qu'ils sont victimes indirecte (témoins) et secondaire (perception) . Il serait non négligeable d'élargir à d'autres structures ces accompagnements et ces recherches.

En cybersécurité, la première faille à combler c'est peut être le silence autour de la souffrance...

Annexe: le retour visuel du sondage





Détail des réponses

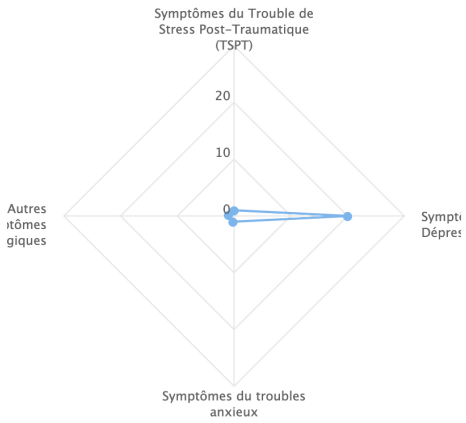
Etat psychologique après une attaque cyber en milieu professionnel, il ne faut pas ignorer!

Répondant n°3

17/03/2025 10:12

14 minutes et 23 secondes

Catégorie	Score
Symptômes du Trouble de Stress Post-Traumatique (TSPT)	1/157
Symptômes Dépressifs	20/157
Symptômes du troubles anxieux	1/138
Autres Symptômes Psychologiques	1/100



attaque cy
profession
3.pdf
92,1 Ko • OK

Etat psych
attaque cy
profession
4.pdf
92,6 Ko • OK

Détail des réponses

Etat psychologique après une attaque cyber en milieu professionnel, il ne faut pas ignorer!

Exporter en PDF

Répondant n°4

17/03/2025 17:03

6 minutes et 31 secondes

Catégorie	Score
Symptômes du Trouble de Stress Post-Traumatique (TSPT)	20/157
Symptômes Dépressifs	1/157
Symptômes du troubles anxieux	1/138
Autres Symptômes Psychologiques	1/100