Cyber stress

Une grande étude sur le stress des Responsables Cyber

Septembre 2021

Advens CYBERSECURITY

CESIN

Sommaire

1

En synthèse

Advens et le CESIN se sont engagés, au second trimestre 2021, dans la réalisation d'une étude sur le stress des métiers de la Cyber, plus précisément, sur le métier de Responsable en Cybersécurité, recouvrant principalement les fonctions de Directeur Cybersécurité ou de RSSI.

Advens a proposé cette initiative, après avoir lu que des études Outre-Atlantique et Outre-Manche faisaient un constat alarmant des niveaux de stress dans lesquels se trouvaient les responsables cybersécurité dans ces pays.

Le CESIN et Advens ont alors construit une enquête destinée à un public français, sur laquelle les membres du CESIN ont naturellement été interrogés. Cette enquête a été conçue par le CESIN et Advens, avec le concours de praticiens, un coach et un oncologue, non spécialistes de la profession Cyber, mais en capacité d'apporter toute leur expérience dans le traitement du stress en contextes exigeants.

L'enquête a permis de collecter les réponses de 330 membres du CESIN, dont 60% de RSSI et 20% de Directeurs Cybersécurité. Tous les secteurs d'activité et tailles d'entreprises ont été couverts, ce qui a permis de constituer un échantillon significatif de ces professions en France.

L'enquête a comporté deux séries de questions. Une première série de 10 questions alignées sur un modèle de mesure international et reconnu de la perception du stress, la Perceived Stress Scale (PSS), et dont l'objet est la détermination du niveau de stress ressenti. Et une série de 22 questions permettant de déterminer les facteurs propres aux métiers de la Cyber et susceptibles de contribuer au stress.

Les réponses aux 10 premières questions permettent de calculer un score sur l'échelle PSS utilisée, qui s'étale de 0 à 40, Le stress est jugé positif ou stimulant si le score est inférieur à 16 (zone « verte »). Entre 16 et 24 (zone « orange »), le score traduit qu'il existe des sentiments d'impuissance occasionnels et des perturbations émotionnelles - certaines situations deviennent difficiles à gérer. Au-delà d'un score de 22 (zone « rouge »), on se situe dans une « zone rouge » accompagnée de risques accrus pour la santé physique et mentale, et un sentiment de menace et d'impuissance.

La mesure du niveau de stress auprès des 330 répondants a conduit à établir un niveau moyen de 18,4. Cela traduit un niveau collectif de stress élevé, comparé à ceux obtenus par d'autres études adressant un panel de métiers large parmi les cadres et ingénieurs. 130 personnes (soit 39% des répondants) sont dans la zone verte. Et 61%

des répondants sont soit en zone orange (33%) soit en zone rouge (28%), et subissent donc un stress aux effets négatifs. Parmi les 92 personnes qui se trouvent en zone rouge, 62 personnes sont en risque de burnout. 22 personnes étant même dans une zone à risque de dépression clinique, avec un score supérieur à 28 sur 40.

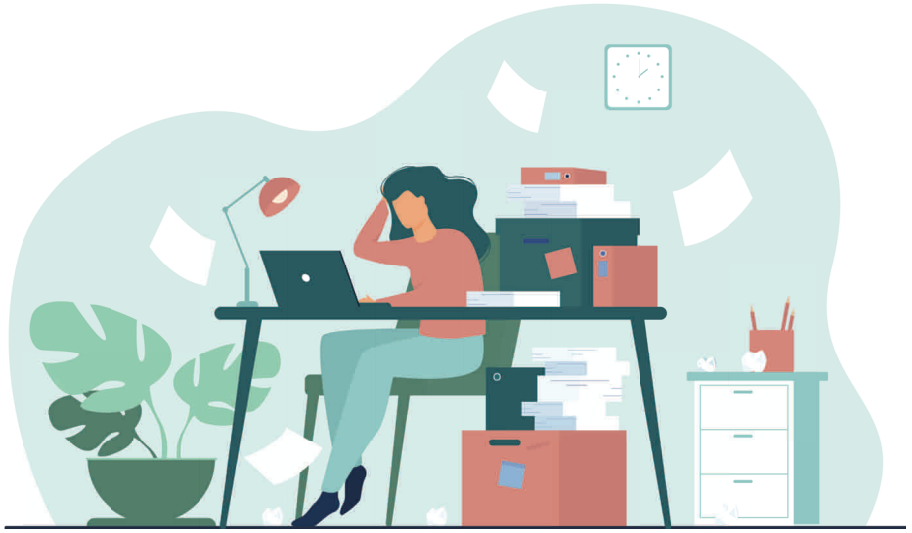
Ces niveaux de stress sont préoccupants. Un stress élevé peut être supportable sur une durée courte. Mais dans la durée, un niveau de stress important peut impacter sérieusement la santé mentale. Et à court terme, un stress répété peut impacter la performance des responsables Cyber et, in fine, la performance des dispositifs de Cybersécurité.

C'est pourquoi l'étude de ce sujet doit être poursuivie, avec notamment une mesure régulière des indicateurs de stress, pour confirmer si les niveaux observés sont inscrits dans la durée. Il est également important de refaire des mesures à distance de la situation pandémique, qui a tendance à majorer le stress pour un grand nombre de professions. Celles de la Cyber ont plutôt été soumises à une aggravation des menaces, depuis le début de la pandémie, et l'isolement forcé lié aux phases de confinement peut avoir accentué la sensation d'impuissance et de découragement devant ces menaces.

En ce qui concerne les facteurs contribuant au stress, les 22 questions posées ont été organisées suivant une typologie de 8 familles caractéristiques des métiers de la cyber : coercition et surveillance, complexité et évolutivité, transversalité, combat et adversité, incertitude et inconnu, gestion de crise, communication et conviction, responsabilité et culpabilité. La majorité de ces 22 questions, 17 sur 22, mettent en évidence des facteurs contributifs du stress, alors que 5 questions sur 22 portent sur des facteurs qui ne semblent pas augmenter le niveau de stress.

Parmi les facteurs les plus contributifs du stress, se trouvent notamment le contexte d'adversité, la difficulté à déconnecter et faire un break, la relation à la responsabilité et la culpabilité et le sentiment d'incertitude et d'inconnu au quotidien. À cela s'ajoutent les évolutions permanentes de la fonction. Les personnes les plus touchées par le stress éprouvent un sentiment d'impuissance et de découragement devant la puissance des attaques. Autre élément notable, la majorité des répondants expriment le risque de perdre leur poste, en cas de crise majeure.

Plus précisément, 82% des répondants confirment exercer dans un contexte d'adversité, face à des ennemis souvent invisibles, 52% des répondants se sentent en permanence sur le qui-vive, près d'un quart des répondants ne se font pas aux aléas et imprévus du métier et 28% se sentent même découragés devant l'augmentation de la fréquence et de la puissance des cyberattaques. En termes de compétences, 60% des répondants pensent posséder l'expertise technique et méthodologique nécessaire et seulement la moitié des répondants estiment avoir la capacité à s'adapter au contexte très évolutif du métier. La gestion des risques, en amont des processus Cyber, est un exercice jugé difficile par 62% des répondants, mais 84% d'entre eux vivent plutôt bien la gestion de crises cyber, en aval. Enfin 38% des répondants déclarent que leur métier souffre « encore » d'un a priori plutôt négatif, 47% se sentent encore incompris, voire jugés parfois excessifs et 54% estiment qu'une crise majeure pourrait leur coûter leur poste. Ce dernier chiffre passe à 65% pour les répondants de la zone rouge.



Certaines réponses confirment que les les Responsables Cyber sont à l'aise avec les valeurs de leur métier. Parmi les situations plutôt bien vécues, ils ne se sentent pas personnellement en danger, ne sont pas gênés par les secrets parfois délicats qu'ils sont amenés à détenir, vivent plutôt bien le fait d'être du côté de la défense sans pouvoir riposter, et se sentent soutenus par leurs proches dans les moments extrêmes de gestion de crise.

Certaines composantes du métier de Responsable Cyber sont manifestement génératrices d'un stress, qui peut parfois devenir négatif. Si certains facteurs semblent

difficiles à maitriser, comme l'intensité des attaques ou leur caractère aléatoire, certains paramètres peuvent être travaillés. Tout cela souligne la richesse des enseignements de cette enquête. Cela incite à poursuivre l'exercice d'analyse, en l'approfondissant sur certains sujets, que ce soit sur l'origine ou sur les impacts de ce stress sur la performance, mais aussi en le pérennisant via une mesure annuelle afin d'observer des tendances. Les métiers de la Cybersécurité étant encore en forte évolution, parfois même naissant dans certaines organisations, il est probable que certains facteurs s'atténuent avec le temps lorsqu'une certaine forme de stabilité sera atteinte.

En ce qui concerne les réponses au stress, plusieurs pistes sont examinées et portent soit sur la modification des causes du stress, soit sur l'atténuation des conséquences. Ces pistes peuvent s'inscrire dans le cadre de communautés telles que le CESIN, à travers des ateliers de « résilience face au stress » ou des séminaires ad hoc. Ces travaux pourront se poursuivre avec une approche plus holistique. Par exemple, la réalisation de portraits complets de professionnels de la Cyber permettrait de mieux comprendre dans sa globalité le sujet du stress, à travers différents parcours.

Au-delà des communautés, la prise en compte du stress doit être faite par l'employer. Elle doit commencer dès l'élaboration de la fiche de poste, être intégrée au parcours de formation et s'appuyer sur des échanges avec les autres métiers de l'entreprise pour une meilleure connaissance et compréhension du métier – ce qui, au passage, ne peut qu'accroitre la sensibilisation aux risques Cyber et le niveau collectif de préparation face à une attaque. Le monde académique a également un rôle à jouer dans l'identification et l'intégration des aspects liés au stress dans l'éducation des professionnels et futurs professionnels.

Comprendre et adresser le sujet du stress chez les professionnels de la Cyber est une démarche doublement gagnante. Il est important d'assurer enthousiasme, épanouissement et équilibre des populations concernées. Mais traiter le stress est une aussi approche qui fera gagner en performance. En travaillant sur les causes du stress, la cybersécurité progressera. D'une part les personnes qui la pilotent se sentiront mieux armés et mieux soutenus. Et d'autre part ce sujet stratégique sera mieux intégré dans la vie numérique de l'entreprise, avec des responsables Cyber correctement reconnus et dotés des bons leviers pour exercer leur fonction.

2

Introduction / Édito

Le risque Cyber, traduisant une atteinte à la sécurité de l'information et des systèmes d'information figure désormais en tête de nombreux classements des risques. En 2021 l'assureur Allianz le place en première position de son baromètre annuel des risques. De même, le Word Economic Forum identifie le risque Cyber dans son top 5 des « dangers clairs et présents ».

Les régulateurs, les assureurs et bon nombre d'organes de contrôle et de veille ont clairement pris la mesure de ce risque. Par ailleurs, avec l'interdépendance entre les organisations, leurs fournisseurs et leurs clients, le risque Cyber est devenu systémique. Les attaques récentes sur des éditeurs de logiciel comme Solarwinds et Kaseya le démontrent aisément.

Mais alors, faut-il encore rappeler que la menace Cyber plane sur toutes les organisations, publiques et privées, peu importe leur taille, compte-tenu de la dépendance accrue au numérique et du caractère extrêmement lucratif de la cybercriminalité ?

Malheureusement oui ! Malgré ce caractère critique et stratégique, malgré les conséquences destructrices, force est de constater qu'il est difficile de traiter ce risque. Ce challenge est celui de toutes les organisations, et il est piloté par une femme ou un homme, en charge de cette problématique. Appelé RSSI (Responsable de la Sécurité des Systèmes d'Information), Directeur / Directrice Cybersécurité ou CISO (Chief Information Security Officer), cette personne a la charge d'orchestrer toutes les actions concourant à la maitrise de ce risque Cyber.

La montée en puissance du sujet Cyber a fait vivre à ces professionnels de la sécurité numérique de grands changements, pour ne pas dire bouleversements au cours des dernières années. Les causes sont tout aussi multiples que le sont les facteurs de complexité de maitrise de ce risque bien particulier. Les conséquences sur le métier et les Femmes et les Hommes qui l'endossent le sont tout autant, sinon plus.

Le CESIN et Advens ont souhaité lancer une grande enquête sur le stress chez les RSSI, Directeurs Cybersécurité et professionnels de la cybersécurité en entreprises ou en administrations. Face à ces mutations, il a semblé important de se demander comment vont ces professionnels, et s'ils parviennent à vivre sereinement leur métier qui se transforme, s'étend et se structure sous la pression du feu croissant des cyberattaques.

Plusieurs éléments sont en train de se redessiner dans la façon dont s'exerce ce métier, ce qui peut donner parfois un sentiment

de vertige, voire de déséquilibre. Les professionnels deviennent plus nombreux, même si à court terme les ressources sont encore insuffisantes. Des spécialités apparaissent, traduisant la richesse des métiers de la Cyber, la palette s'est élargie avec un curseur qui a bougé vers davantage de détection et de réponse à incidents. Pour certains, le quotidien est de plus en plus marqué par les activités très opérationnelles et la gestion de crises.

La problématique Cyber est de mieux en mieux comprise et adressée par le « top management » des entreprises. Mais le temps pour se poser, construire et anticiper, est toujours plus court.

Est-ce que tous les professionnels de la cybersécurité sont taillés pour des aventures souvent mouvementées ? Arrivent-ils à prendre le recul nécessaire pour être de bons stratèges, tout en composant avec un quotidien qui réclame toujours plus d'énergie et d'efficacité ? Est-ce que ce métier leur pèse ou est-ce qu'il les stimule et les enthousiasme ? Comment vivent-ils la relation avec leurs proches, leurs familles, leurs collègues et leur manager ?

Autant de sujets qui ont encore été peu analysés, car ce métier est jeune et il vit de nombreuses mutations depuis quelques années.

Les médias font désormais une « belle place » à la cybersécurité. Il était temps de prendre soin de ceux qui font la sécurité, et d'écouter leur ressenti sur ce métier exigeant.

Mylène JAROSSAY, CESIN
& Benjamin LEROUX, Advens

3

Les mots pour le dire
Rappel de la démarche d'étude

3.1- La genèse

Cette étude est née en réaction à une série d'articles publiés sur des médias anglo-saxons autour de la santé mentale des RSSI ou Directeurs Cybersécurité, appelés CISO outre-Manche et outre-Atlantique. Ces contenus, parus entre début 2019 et début 2020, agitaient le spectre de responsables Cyber en pleine crise : burn-out, dépression, consommation excessive de médicaments, d'alcools et autres substances. Manifestement la coupe était pleine et la situation des plus graves !

Comment savoir ce que traduisaient réellement ces articles aux titres parfois racoleurs ? Comment importer ces éléments sur les territoires européens ou français ? Peut-on appliquer les conclusions aux responsables Cyber français ? Les cultures d'entreprise, le droit du travail, le contexte socio-professionnel et bien d'autres facteurs semblent trop différents pour se permettre de faire un « copier / coller » de ces résultats. Pour autant la problématique Cyber est globale. Et toutes les solutions pour faire face aux risques psycho-sociaux chez les responsables Cyber sont bonnes à prendre.

Le sujet de la santé mentale au travail est intéressant et relativement nouveau pour la communauté française. Les thèmes de la gestion du stress, de la résilience émotionnelle et de la charge mentale sont plus que jamais dans l'air du temps depuis 2020, le début de la pandémie COVID et après les premiers mois de confinement.

Ainsi est née cette étude sous l'impulsion d'Advens, qui s'est associé au CESIN pour concevoir et conduire cette étude. Quid du stress des Responsables Cyber en France ? Y a-t-il un sujet ? Que peut-on en dire ? Le plus simple était de poser la question aux intéressés. Et exploiter ainsi la puissance et la solidarité du CESIN et de ses centaines de membres pour tenter de trouver des réponses et d'établir un état des lieux.

3.2- La démarche d'étude

Cette étude s'est construite autour d'une enquête à destination des principaux intéressés, à savoir les RSSI et directeurs / directrices Cyber des entreprises privées et structures publiques de France. Pour les toucher, le CESIN a été une évidence. L'association regroupe des profils issus d'horizons très variés, intervenant dans des secteurs tout aussi variés, dans des organisations aux tailles et aux enjeux divers. Cela a permis d'éviter le biais de ne se concentrer que sur les groupes et entreprises multinationales, par exemple.

L'étude s'est appuyée sur une enquête, composée de deux questionnaires qui seront détaillés ci-après. Il est important de souligner un élément clé de la démarche d'étude : le concours d'intervenants externes ayant une expertise ou une expérience en matière de gestion du stress, aussi bien dans la phase de conception de l'enquête que pour l'analyse de ses résultats. En effet, si les initiateurs de cette étude peuvent prétendre à une certaine expertise sur les questions Cyber, il n'en est rien sur les sujets de la santé mentale, de la résistance au stress et des thématiques associées.

C'est pourquoi les résultats de l'enquête n'ont pas seulement été analysés par des habitués de la Cyber. Bien au contraire. Ils ont été minutieusement analysés par des intervenants qui seront présentés dans le paragraphe suivant. Et il se trouve que la Cyber a représenté un contexte d'étude qui a passionné ces intervenants !

L'enquête est basée sur deux séries de questions, qui ont été rassemblées en un questionnaire unique auquel ont répondu intégralement les différentes personnes interrogées et volontaires pour répondre.

→ La première série de questions a pour objectif d'analyser le niveau de stress que perçoivent les responsables Cyber. La perception du stress est propre à chacun, les mêmes conditions ne déclenchent pas le même niveau de stress ressenti par les uns et les autres. Il appartient donc à chacun d'estimer une position sur une échelle de stress vécu, par analogie avec l'évaluation de l'intensité de la douleur sur des échelles proposées par des médecins spécialistes de la lutte contre la douleur. Cette partie comporte dix questions et est issue d'un modèle de mesure de la perception du stress, la Perceived Stress Scale (PSS). Les résultats de ce volet sont abordés en partie 4.

→ La seconde série de questions consiste à identifier les spécificités du métier qui pourraient être à l'origine du stress ressenti. Il s'agit de comprendre ce qui cause le stress ressenti, au travers du prisme du métier. Les facteurs personnels (la situation familiale par exemple) ou professionnels plus larges (les relations avec les collègues ou la hiérarchie, la trajectoire de carrière, la santé de l'entreprise, etc.) ne sont pas pris en compte. Est analysée une série de critères considérés comme caractéristiques du métier de responsable Cyber. Les conclusions intermédiaires liées à ce volet sont partagées en partie 5.

L'étude cherche à évaluer l'existence d'un sujet de préoccupation autour du stress provoqué par les caractéristiques propres au métier de responsables Cyber ; et indirectement le degré d'importance que la communauté Cyber doit y accorder. En cas de problématique avérée, et quel que soit le niveau d'intensité de ce stress, les solutions ne sont pas comprises dans le périmètre de ces travaux. Quelques pistes sont tout de même abordées en partie 7, notamment grâce au concours des intervenants externes.

3.3- Les intervenants

Mylène JAROSSAY

Mylène Jarossay est Directrice Cybersécurité du Groupe LVMH et Présidente du CESIN.
Ingénieure en Informatique & Réseaux de formation, Mylène a travaillé dans des secteurs divers, d'abord chez l'éditeur de logiciels Prologue Software, ensuite dans le secteur Défense, puis dans le domaine de la santé, à l'Institut Curie tant que DSI Adjointe et RSSI. En 2015, elle a rejoint le Groupe LVMH, leader mondial du luxe, dont elle est la Directrice Cybersécurité.
Elle a été l'un des fondateurs du CESIN en 2012.

Benjamin LEROUX

Benjamin Leroux est Directeur Marketing et RSSI chez Advens. Il évolue dans le milieu de la cybersécurité depuis plus de 15 ans. Après des expériences au sein du cabinet Accenture puis de la société Dictao (Idemia), il a occupé un poste de RSSI Groupe pour un acteur des services financiers. Il a rejoint Advens en 2012 pour développer les offres de conseil et d'accompagnement RSSI. Il est désormais en charge de la définition et de l'animation de l'ensemble des offres d'Advens et du catalogue de services associé - pour rendre la sécurité plus accessible, plus agile et plus efficace. Benjamin représente Advens au CESIN, au CLUSIF et dans d'autres groupes professionnels. Il pilote également la stratégie de sécurité et de conformité de la société Advens.

Alain LIVARTOWSKI

Le Dr Alain Livartowski est oncologue à l'Institut Curie, spécialisé dans le traitement des cancers du poumon.
Il a été très impliqué dans la construction du Système d'Information de l'Institut Curie, dans sa stratégie du « tout numérique » en soutien à l'ensemble des activités et processus hospitaliers. Il contribue également à la nouvelle Direction des Data dont l'objectif principal est, à travers l'analyse des données cliniques et de recherche, de permettre de découvrir de nouvelles pistes thérapeutiques et d'optimiser le diagnostic des cancers.
Alain a travaillé sur les conséquences psychologiques chez les soignants qui prennent en charge des patients atteints de cancer et les risques de « burn out »

Yann OFANOWSKI

Coach et praticien ANC (Approche Neurocognitive Comportementale), Yann Ofanowski accompagne les dirigeants dans leur quête d'efficacité et de sérénité, au sein d'univers complexes et stressants.
Il aide les dirigeants à repenser leur cadre mental, à développer leur agilité émotionnelle, leur autonomie affective, leur rapport à la performance.
Avant de devenir coach, il a passé 20 ans chez Accenture, d'abord dans le conseil puis en interne comme directeur RH. Il est ingénieur de formation, père de 3 enfants et artiste plasticien passionné.
En parallèle de son activité en entreprise, il enseigne le leadership à l'IESEG School of Management (à Lille).

3.4- Le panel de répondants

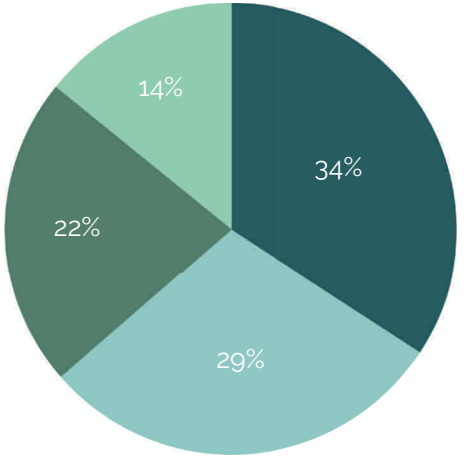
330 managers Cyber ont répondu à l'enquête.

Entreprises « clientes »

La cible de l'enquête a été d'interroger les membres actifs du CESIN. Les membres actifs sont des spécialistes occupant des postes de management de la sécurité de l'information et du numérique, au sein d'entreprises privées ou publiques. Sont ainsi exclues les entreprises commerciales dont l'activité principale est la fourniture de solutions et/ou de prestations en sécurité de l'information et du numérique.

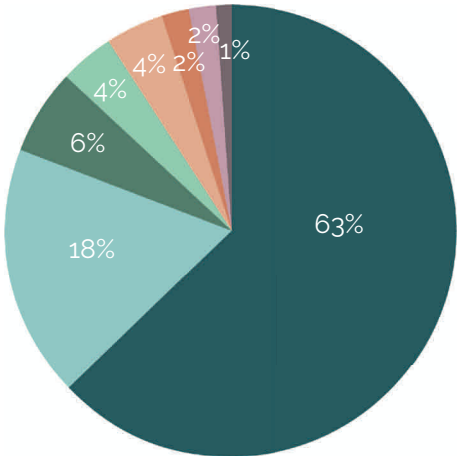
Taille des entreprises

Les répondants sont issus de structures de tailles variées.



Taille de l'entreprise des répondants

- 1 000 à 10 000 employés
- 10 000 à 100 000 employés
- Moins de 1 000 employés
- Plus de 100 000 employés



Métiers des répondants

- RSSI
- Directeur cybersécurité
- Autre
- Expert cybersécurité
- DSI
- Responsable SOC et/ou CERT/CSIRT
- Risk manager
- Architecte cybersécurité

Les deux-tiers des répondants (63%) exercent le métier de RSSI, 18% sont des Directeurs Cybersécurité.

À propos du genre

L'enquête n'a pas collecté le genre des répondants. Mais il est probable qu'environ 90% des répondants soient des hommes, ce qui correspond au taux actuel d'hommes parmi les membres du CESIN.

Or des études montrent que les hommes admettent plus difficilement ou plus tardivement être soumis à une pression ou en situation de stress. Cela peut introduire un biais de minimisation du stress ressenti.

À ce sujet Rachel Liu, fondatrice de Human Tempo, nous précise « *les hommes que nous recevons sont en général bien plus dans le déni, et bien plus « cabossés » que les femmes lorsqu'ils acceptent enfin d'agir. Par exemple, une majorité des hommes que nous recevons ont eu des pensées suicidaires, alors que c'est le cas pour une minorité de femmes.* »

3.5- Études similaires

Le sujet du stress des responsables Cyber ne semble pas avoir été abordé à l'échelle française. En Europe et même aux Etats-Unis, on cite souvent les rapports rédigés par la société anglaise Nominet[1] et diffusé en février 2020 pour le dernier. Sur le premier trimestre 2020, cette étude a été reprise par plusieurs media français, et ce sans préciser toujours clairement que le panel ne concernait que le Royaume-Uni. Le stress des Responsables Cyber français, comme sujet d'étude, est donc inédit.

Plus globalement, le facteur humain est souvent abordé en matière de cybersécurité. Mais il est quasiment toujours destiné à traiter la dimension humaine, plutôt comportementale, dans les failles de sécurité et ne concerne pas les humains qui « font » la cybersécurité.

Cependant certaines thématiques connexes et relatives à ces humains ont émergé ces dernières années. Outre-Atlantique, et dans certains cercles assez techniques, le sujet a été traité sous l'angle de la « communauté ». C'est une catégorie qui a fait son apparition dans le programme de la célèbre conférence Black Hat depuis 2018[2]. Cette année-là, de nombreux sujets « nouveaux » ont été abordés, tels que :

→ La santé mentale dans la communauté des hackers : https://www.blackhat.com/us-18/briefings/schedule/#mental-health-hacks-fighting-burnout-depression-and-suicide-in-the-hacker-community-10659

1- https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf
2- https://www.blackhat.com/us-18/briefings/schedule/#track/community

→ L'addiction dans le milieu de la sécurité de l'information : https://www.blackhat.com/us-18/briefings/schedule/#holding-on-for-tonight-addiction-in-infosec-10951

→ Le stress cognitif dans les opérations tactiques de sécurité : https://www.blackhat.com/us-18/briefings/schedule/#stress-and-hacking-understanding-cognitive-stress-in-tactical-cyber-ops-10243

Une étude en 2020 a, par ailleurs, étudié le profil psychologique des hackers white/grey/black hats :

→ Article « Psychological Profiling of Hacking Potential », Proceedings of the 53rd Hawaii issu de l'International Conference on System Sciences 2020 :

→ https://www.researchgate.net/publication/339029249_Psychological_Profiling_of_Hacking_Potential

Il est à noter que l'ANSSI et la DGEFP, en collaboration avec l'AFPA, ont lancé une enquête sur les professionnels de la cybersécurité, dans la continuité de leurs travaux autour du Panorama des métiers de la cybersécurité, travaux auxquels le CESIN a contribué. Ceux-ci ont permis d'apporter une spécification claire et actualisée des différents métiers de la cybersécurité. L'enquête qui a suivi, quant à elle, comportait, entre autres, une question sur le niveau de stress ressenti. Les conclusions de cette enquête seront publiées à l'automne 2021, mais il apparait d'ores et déjà que l'indicateur unique de stress collecté dans cette enquête soit en adéquation avec la présente étude, avec une typologie de répondants différente du périmètre couvert par l'enquête CESIN-Advens, car toutes sortes de métiers de la Cyber étaient interrogées.

Au-delà de ces problématiques similaires au sujet de la présente

étude, la communauté s'est penchée sur des sujets qui font encore beaucoup réagir en 2021 comme la place des femmes dans la cybersécurité mais également l'inclusion et les profils « hors cadre », tels que les autistes et les Hauts Potentiels. Ce sujet de l'inclusion fait désormais l'objet de travaux menés[3] par Advens et le CESIN. Les thématiques de l'inclusion et ce dans différentes régions du monde ont été régulièrement abordées lors des autres éditions de cette conférence.

Une autre thématique notable pourrait être celle de la « Cyber fatigue », dont les premières occurrences sont issues d'un document du cabinet KPMG paru en 2016[4]. Ce concept désigne le mouvement « d'abandon d'une défense proactive face à des attaquants multiples ». Il semble cependant s'appliquer plutôt à une organisation qu'à un individu. Il est souvent associé aux problématiques du SOC et de la multiplicité des technologies à maitriser pour détecter et traiter correctement les incidents. Il n'est pas lié à l'état ni à la santé mentale des professionnels du domaine.

3- https://www.advens.fr/fr/ressources/blog/tech-cyber-comment-rendre-la-cyber-plus-inclusive
4- https://assets.kpmg/content/dam/kpmg/ch/pdf/ch-cyber-fatigue-en.pdf

4

Connais-toi toi-même
Évaluation du stress perçu

4.1- Rationnel et irrationnel

L'étude a pour objectif initial d'identifier l'existence, ou non, d'une problématique relative aux stress des professionnels de la cybersécurité et liée à la nature de leur métier. Si la plupart des personnes interrogées ne ressentent pas les effets d'un stress négatif, le sujet ne nécessitera sans doute pas une analyse plus en profondeur.

Il est donc primordial de commencer par mesurer le niveau de stress ressenti par les responsables Cyber interrogés. C'est l'objet de la première partie de l'enquête. Le premier enjeu, pour ce faire, a été le choix de la méthode. Le sujet étant lié à un stress ressenti, par nature propre à chaque personne interrogée, il était nécessaire de définir une approche rationnelle et idéalement universelle, facilitant la comparaison et intégrant les biais de perception.

Pour y parvenir, l'apport des intervenants externes a été plus que bénéfique et a permis le recours à une méthode reconnue dans le domaine de l'évaluation du stress. Cette méthode a fait l'objet de la première partie du questionnaire, dont on retrouve les questions dans la section suivante et les résultats détaillés en annexe.

4.2- Échelle de mesure du stress

Depuis que les chercheurs se sont intéressés à l'évaluation du stress, les méthodes ont évolué car la conception même du stress s'est modifiée. Dans les années 80, les chercheurs se sont aperçus que l'impact d'une situation supposée stressante n'était pas le même selon les personnes et surtout que « l'évaluation que l'individu portait sur cette situation était déterminante sur son vécu » (Lindsay & Norman, 1980).

En 1983, Cohen, Kamarck, et Mermelstein proposent un questionnaire de stress perçu basé sur le modèle théorique transactionnel : la Perceived Stress Scale (PSS) a pour objectif « d'évaluer le degré selon lequel les personnes interrogées estiment que leur vie est imprévisible, incontrôlable et surchargée. » La PSS permet d'évaluer d'une façon globale si une personne estime avoir la capacité à faire face ou non à des événements ou à des moments difficiles à vivre, sans toutefois les spécifier. Cohen, Kamarck, et Mermelstein (1983) présentent trois versions, en 14, 10 et 4 items sous les appellations de PSS14, PSS10 et PSS4.

Ces modèles ont été utilisés dans de nombreux pays et déclinés dans le monde professionnel. La version française du PSS10 a fait l'objet de plusieurs études et sa

fiabilité/corrélation avec d'autres modèles de référence a été démontrée.

Dans le cadre de cette étude auprès des responsables Cyber, sont incluses les 10 questions du PSS10 parmi les 35 questions posées.

	Questions PSS10
1	Au cours du dernier mois vous êtes-vous senti contrarié ou énervé par des événements non prévus ?
2	Au cours du dernier mois vous êtes-vous senti incapable de contrôler les « fondamentaux » de votre métier/fonction/rôle ?
3	Au cours du dernier mois vous êtes-vous senti(e) nerveux(se) ou stressé(e) ?
4	Au cours du dernier mois vous êtes-vous senti(e) pleinement capable de gérer vos problèmes professionnels ?
5	Au cours du dernier mois avez-vous senti que les choses allaient comme vous le vouliez ?
6	Au cours du dernier mois avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?
7	Au cours du dernier mois avez-vous été capable de maîtriser (intérieurement et extérieurement) votre agacement ?
8	Au cours du dernier mois avez-vous senti que vous « maîtrisiez la situation » ?
9	Au cours du dernier mois vous êtes-vous senti(e) irrité(e) parce que les événements échappaient à vôtre contrôle ?
10	Au cours du dernier mois avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?

Les réponses aux questions sont évaluées entre 0 (Stress bas) et 4 (Stress élevé). Dans le cadre de l'étude, les points sont attribués selon l'échelle suivante :

→ Jamais = 0,

→ Presque Jamais = 1,

→ Parfois = 2,

→ Assez Souvent = 3,

→ Souvent = 4.

Ceci est valable pour toutes les questions sauf pour les quatre dites « inversées » (Q6, Q7, Q9, Q10) ou Jamais = 4, Presque Jamais = 3 etc. En additionnant les scores des 10 questions, nous obtenons un total compris entre 0 et 40 pour chaque participant.

4.3- Partage des résultats

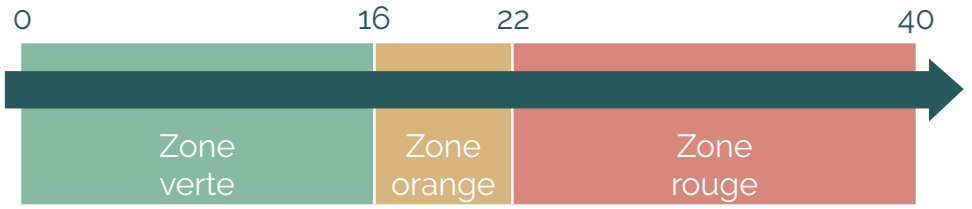
Le résultat moyen par question est exposé dans le tableau suivant

	Questions PSS10	Moyenne des réponses
1	Au cours du dernier mois vous êtes-vous senti contrarié ou énervé par des événements non prévus ?	2,63
2	Au cours du dernier mois vous êtes-vous senti incapable de contrôler les « fondamentaux » de votre métier/fonction/rôle ?	2,12
3	Au cours du dernier mois vous êtes-vous senti(e) nerveux(se) ou stressé(e) ?	2,58
4	Au cours du dernier mois vous êtes-vous senti(e) pleinement capable de gérer vos problèmes professionnels ?	1,04
5	Au cours du dernier mois avez-vous senti que les choses allaient comme vous le vouliez ?	1,47
6	Au cours du dernier mois avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?	2,53

7	Au cours du dernier mois avez-vous été capable de maîtriser (intérieurement et extérieurement) votre agacement ?	0,93
8	Au cours du dernier mois avez-vous senti que vous « maîtrisiez la situation » ?	1,40
9	Au cours du dernier mois vous êtes-vous senti(e) irrité(e) parce que les événements échappaient à vôtre contrôle ?	1,99
10	Au cours du dernier mois avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?	1,72
	Total	**18,41**

Le score moyen sur le panel est de **18,4**. Cela constitue un **niveau collectif élevé**. En effet, comme indiqué dans les graphiques ci-dessous, un score de 16/40 représente le point d'inflexion entre un stress stimulant et un stress commençant à provoquer des désagréments émotionnels et comportementaux. Un score de 22/40 représente le passage dans une zone à risque pour la santé physique et psychique.

Zone verte	**Entre 0 et 16**	De calme à stress « stimulant » ou « positif »
Zone orange	**Entre 16 et 22**	Sentiment d'impuissance occasionnel entraînant des perturbations émotionnelles, situations parfois difficiles à gérer
Zone rouge	**>22**	Fort sentiment d'impuissance, sensation plus ou moins diffuse de menace, risques sur la santé physique et mentale (pression sanguine, IMC, efficacité immunitaire, troubles du sommeil, addictions...)

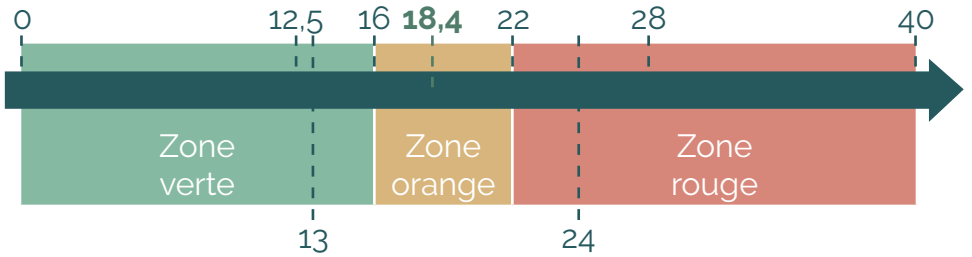


Si l'on remet en perspective les résultats avec des données normatives, on souligne le niveau collectif élevé.

En 1988, l'étude fondatrice de Cohen et Williamson portant sur un panel d'environ 3000 citoyens américains a permis d'établir une « norme de stress » située à 12,5. Selon les classes sociales, sexe, niveau d'étude etc. les scores moyens varient entre 11 et 15.

Résultats enquête 2021 CESIN-ADVENS portant sur 330 participants (directeurs Cybersécurité et RSSI).

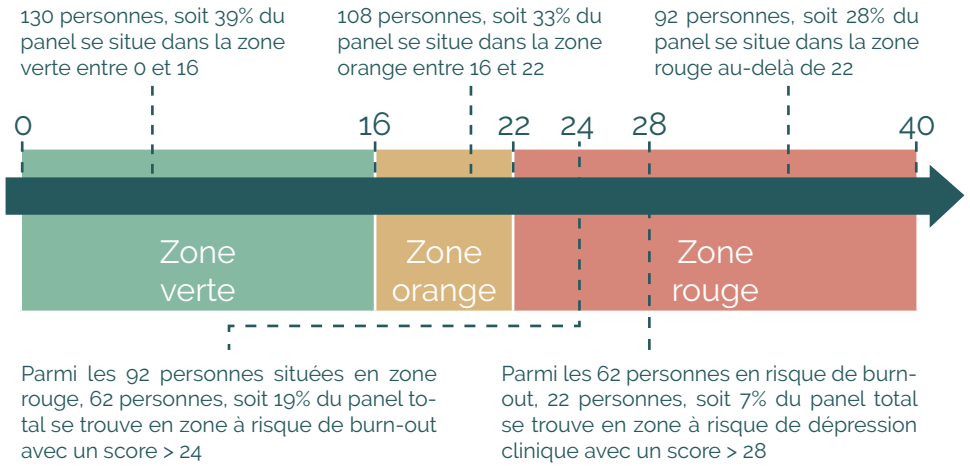
Seuil diagnostique clinique de la dépression (étude 2012 en France portant sur 80000 personnes).



En 2011, des données PSS10 ont été récupérées auprès de 16853 salariés dans 17 grandes entreprises françaises (> 1000 salariés) réparties sur 39 sites. La moyenne s'établit autour de 13, avec un score de 12,2 pour les 8927 cadres/ingénieurs (soit environ 50% du panel). On note un écart de stress perçu entre les 7228 femmes (14,3) et les 9625 hommes (11,7).

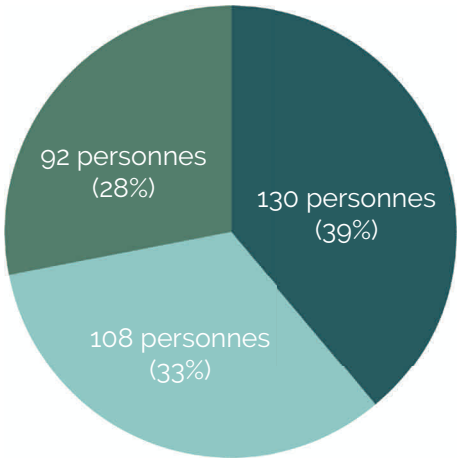
Symptômes de burn-out, diminution des capacités d'empathie, de concentration et de récupération.

Dans le détail, on se rend compte que la grande majorité (61%) des responsables Cyber interrogés subit un stress aux effets négatifs. Ce résultat est très important car il indique que la population observée subit une charge mentale qui provoque une souffrance.



La représentation suivante illustre davantage cette répartition.

Zone verte	**Entre 0 et 16**	Calme. Stress dit « stimulant » ou « positif ».
Zone orange	**Entre 16 et 22**	Sentiment d'impuissance occasionnel entraînant des perturbations émotionnelles, situations parfois difficiles à gérer.
Zone rouge	**>22**	Fort sentiment d'impuissance, sensation plus ou moins diffuse de menace, risques sur la santé physique et mentale (pression sanguine, IMC, efficacité immunitaire, troubles du sommeil, addictions...).

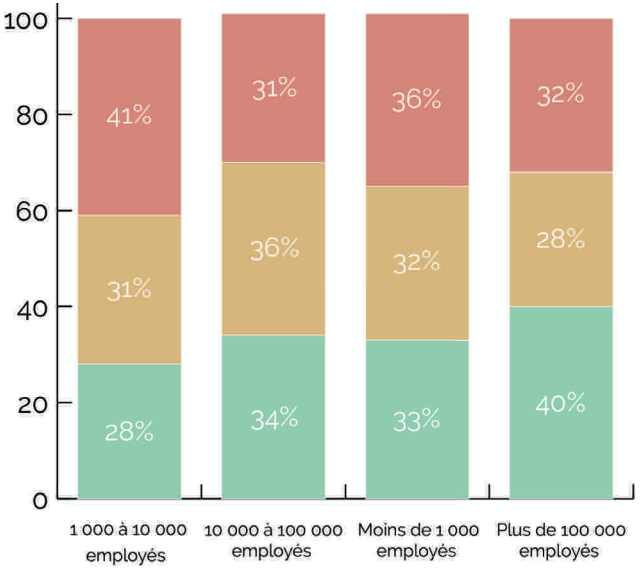


Intensité du stress perçu par les 330 participants

- Stress sous contrôle (PSS10<16)
- Zone de vigilance (16<PSS10<22)
- Zone à risque (22<PSS10)

4.4- Corrélation des résultats

Le niveau de stress est-il corrélé à la taille de l'entreprise ?
Il a été mis en relation la zone (vert, orange, rouge) correspondant au niveau de stress perçu et la taille des entreprises dont sont membres les répondants.



Niveau de stress par rapport à la taille de l'entreprise

	Vert	Orange	Rouge
1000 à 10 000 employés	28%	31%	41%
10 000 à 100 000 employés	34%	36%	31%
Moins de 1000 employés	33%	32%	36%
Plus de 100 000 employés	40%	28%	32%

Les écarts du niveau de stress perçus selon la taille de l'entreprise ne sont pas flagrants. Néanmoins, 62% des personnes qui se situent dans la zone rouge sont dans des entreprises de moins de 10 000 employés, soit un peu plus que le taux de personnes appartenant à cette catégorie d'entreprises (56%).

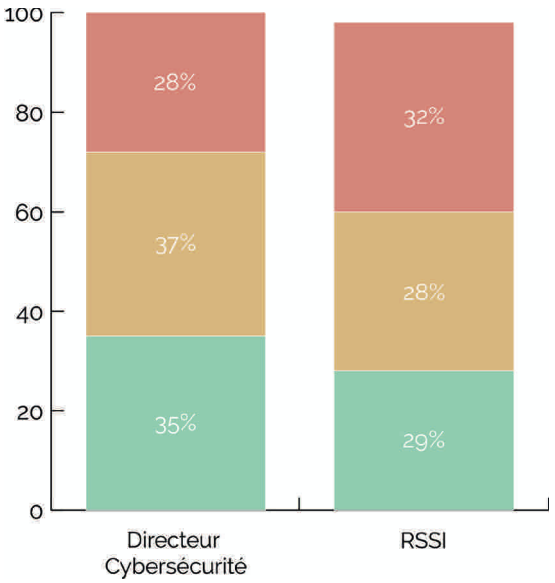
Une explication peut être que dans ces entreprises, il y a encore en général de petites équipes cybersécurité, ce qui, d'une certaine façon, isole ou singularise ceux qui exercent cette fonction au sein de leur entreprise. A cela peut s'ajouter le critère de la maturité. Dans une structure de plus petite taille, il peut arriver que les différentes activités du responsable Cyber ne soient pas totalement légitimées et nécessitent des travaux de prise de conscience, qui peuvent induire une charge mentale.

Le niveau de stress est-il corrélé au métier ?

De même, il a été mis en relation la zone (vert, orange, rouge) correspondant au niveau de stress perçu et le métier exercé par les répondants.

81% des répondants sont soit RSSI, soit Directeurs cybersécurité. Si l'on compare la répartition des niveaux de stress entre ces deux grands métiers représentés dans l'échantillon, on constate que la proportion de personnes dans la zone rouge est plus élevée chez les RSSI.

Les professionnels de la cybersécurité ayant le statut de cadres dirigeants sont soumis, semble-t-il, à un niveau de stress moins élevé. Cela rejoint d'une part l'explication liée à l'analyse précédente sur la dimension du sujet Cyber dans l'entreprise, le Directeur cybersécurité pouvant s'appuyer sur une équipe. Et cela est complété par le fait que le statut de cadre dirigeant constitue une reconnaissance de la place du risque Cyber dans la défense des intérêts de l'entreprise. Pour autant ce statut peut s'accompagner d'une certaine forme de précarité selon la structure (« Le Directeur Cyber saute-t-il en cas de crise ?... »), ce qui pourrait représenter une source de stress.



Niveau de stress par rapport au métier

	Vert	Orange	Rouge
Directeur Cybersécurité	35%	37%	28%
RSSI	29%	32%	38%

Le top 10 des répondants ayant les plus hauts niveaux de stress

Si l'on fait un focus sur les 10 personnes ayant le niveau ressenti de stress le plus élevé parmi les 330 répondants, on constate que ces professionnels ont un **niveau de stress supérieur à 30**, ce qui les classe dans une catégorie très à risque sur le plan de la santé physique et mentale. Le score de stress ressenti **le plus élevé est de 34**.

Parmi ces répondants, 9 sur 10 sont des RSSI et le dixième est un architecte en cybersécurité. Il n'y a pas de Directeur cybersécurité dans cette population.

Si l'on examine les entreprises de ces répondants les plus stressés, 8 entreprises sur 10 ont moins de 10 000 employés, alors que cette taille d'entreprise ne concerne que 56% des répondants. Les deux autres ont soit entre 10 000 et 100 000 employés, soit plus de 100 000 employés.

Les niveaux de stress les plus faibles

Si l'on examine la population de la zone verte, dont le niveau de stress ressenti est inférieur à 16, on retrouve une distribution à peu près équivalente à la distribution globale des répondants quoique légèrement favorable aux Directeurs Cybersécurité (20% dans la zone verte, pour 18% des répondants) et aux experts en cybersécurité (7% dans la zone verte, pour 4% des répondants), par rapport aux RSSI (58% dans la zone verte, pour 63% des répondants).

Les scores les plus élevés parmi les 10 questions

Si l'on observe les questions ayant obtenu le score moyen le plus élevé parmi les dix questions, on voit qu'il est question de contrariété, de nervosité et d'anxiété, mais également le sentiment d'être débordé par l'ensemble des tâches à faire. Cet élément rejoint le sentiment de découragement exprimé dans la deuxième série de questions concernant les facteurs de stress.

5

Un métier à risques
Recherche des facteurs de stress

5.1- Typologie des facteurs de stress

Une fois que le diagnostic est posé sur le niveau de stress ressenti, l'objectif de l'étude est de trouver les facteurs contributifs de ce stress et qui seraient spécifiques du milieu de la Cybersécurité.

En effet, les métiers de la Cybersécurité s'inscrivent globalement dans l'ensemble des métiers du numérique et rencontrent, de façon générale, les difficultés courantes de ces métiers. Au-delà de ces difficultés qui ont déjà été largement étudiées et commentées, l'objectif de la présente étude est de se concentrer sur ce qui constitue les particularités des métiers de la Cybersécurité et qui est susceptible d'éprouver mentalement ces professionnels. Il faut donc déterminer si les facteurs spécifiques de la Cybersécurité sont réellement contributifs du stress ressenti, et si c'est le cas, lesquels sont les plus aggravants. Ceci afin d'orienter la recherche de pistes permettant de traiter et réduire le stress ressenti.

Pour cela, **22 questions** ont été posées pour faire émerger une série de critères spécifiques du métier de la Cybersécurité. Ces questions ont été regroupées en **8 familles de critères** :

1. Coercition et surveillance : le responsable Cyber définit des stratégies de défense qui conduisent,

→ D'une part, à interdire ou bloquer certaines actions effectuées par les employés (qui sont également ses collègues), à titre préventif, ce qui peut le faire apparaître tel un censeur.

→ D'autre part, à collecter et analyser des traces, donc avoir les moyens d'observer les pratiques professionnelles et personnelles des employés (car ceux-ci intègrent une part personnelle dans leur usage des moyens informatiques) et de constater des écarts par rapport à une politique interne ou à des bonnes pratiques, ce qui peut donner lieu à des rappels à l'ordre voire des sanctions. Le responsable Cyber peut alors apparaître alors comme un contrôleur (« big brother ») et un juge.

2. Complexité et évolutivité : la richesse technologique, l'intégration massive de services dans le cloud, les nombreuses attentes des clients internes et externes font des systèmes d'information des organisations actuelles, étendues et hyper-connectées, un terrain complexe à protéger des menaces qui évoluent sans cesse. Cela mène à un contexte riche et changeant, qui requiert un questionnement permanent sur les stratégies à adopter.

3. Transversalité : pour être suffisamment couvrante et efficace, la cyberdéfense doit être omniprésente. Elle doit s'insérer de façon transverse à l'entreprise et à tous les niveaux, dans toutes les architectures, dans tous les composants techniques, dans tous les métiers, en intégrant bien sûr les facteurs humain et organisationnel.

4. Combat et adversité : le manager Cyber est confronté à une situation rare parmi les métiers de l'entreprise, celle de devoir faire face à des adversaires externes et internes de l'entreprise. Une situation qui le place dans un rôle singulier de combattant. Par ailleurs, compte-tenu du niveau de menace actuel et de l'intensité de la cybercriminalité, ce combat est une lutte asymétrique, face à une puissance d'attaque souvent bien supérieure à la capacité de défense d'une organisation donnée.

5. Incertitude et inconnu : l'exercice de la défense est confronté à une incertitude permanente sur le moment et la forme du prochain incident. Ce qui oblige le manager Cyber à être prêt à toute éventualité et à tout moment, car il ne peut jamais considérer qu'il est totalement protégé.

6. Gestion de crise : la gestion de crise est une composante importante des métiers de la cybersécurité. Elle nécessite une disponibilité importante et requiert de proposer et/ou de prendre des décisions sous la pression et sans avoir tous les éléments d'appréciation. Elle s'appuie sur peu de modèles historiques connus. Le manager Cyber gère ses crises en faisant au mieux pour éviter les biais cognitifs qui peuvent parasiter ou paralyser son action.

7. Communication et conviction : parce qu'il s'adresse à de nombreux métiers de l'entreprise pour obtenir leur adhésion et leur contribution, le Responsable Cyber doit savoir communiquer et convaincre sur un domaine pouvant paraître austère, contraignant et faisant appel à un nécessaire effort collectif.

8. Responsabilité et culpabilité : le Responsable Cyber met en œuvre des plans d'action qui demandent des moyens financiers et humains, et sont susceptibles d'imposer des contraintes opérationnelles. L'efficacité de sa démarche est scrutée et jugée. Même si ses stratégies sont pertinentes et d'un très bon niveau pour traiter les risques, l'entreprise ne peut être totalement à l'abri d'une crise ayant un impact significatif. Le manager est donc confronté à deux réactions potentielles de doute et de jugement. S'il ne se passe rien, « à quoi tout cela sert-il vraiment ? » et s'il advient une crise majeure, « tout cela n'a servi à rien ». Un cocktail avec un zeste parfois amer de sentiment d'inutilité et de culpabilité…

Ces différents critères peuvent placer le responsable Cybersécurité dans un contexte de doute, de crainte, d'instabilité, et de questionnement sur ses valeurs. Ils ont donc été pris en compte dans la seconde partie de notre étude relative à l'identification des facteurs contributifs au stress.

5.2- Principaux facteurs de stress

Si l'on examine la moyenne des réponses aux 22 questions relatives à ces critères, on constate que 17 questions obtiennent un résultat en faveur d'une contribution au stress alors que 5 questions concernent des facteurs finalement peu influents sur le stress.
Si l'on évoque ces derniers facteurs, on peut établir des managers Cyber que :

→ Ils sont relativement à l'aise avec les secrets qu'ils détiennent (Q15)

→ Ils ne se sentent pas forcément frustrés de ne pouvoir contre-atta-

quer (Q20) ni de ne pas connaître l'identité des acteurs malveillants (Q25)

→ Ils ne se sentent pas personnellement en danger dans l'exercice de leur métier (Q23),

→ Et ils sont largement compris et soutenus par leurs proches lorsqu'ils sont confrontés à une crise (Q31).

Les familles de critères les plus contributifs au stress sont

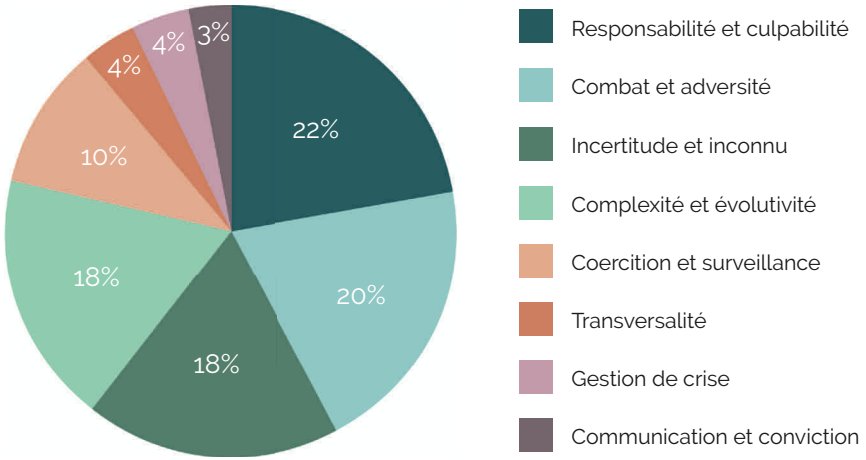
→ la relation à la responsabilité et la culpabilité,

→ le contexte de combat et d'adversité,

→ la part importante d'incertitude et d'inconnu

→ et la complexité et l'évolutivité de la fonction.

Poids respectif des familles de critères contribuant au stress



S'il on examine plus précisément le top 5 des facteurs les plus créateurs de stress, on constate que le sentiment d'adversité est prédominant et que les répondants sont sans cesse sur le qui-vive, sans jamais pouvoir se déconnecter, dans la crainte d'un évènement. Et cette situation d'instabilité est aggravée par le fait que la menace évolue sans cesse et demande une défense tout aussi évolutive. Le métier navigue en terrain hostile, avec un contexte de déséquilibre permanent. Il doit par ailleurs justifier de l'utilité de son action et n'a pas droit à l'erreur car celle-ci peut conduire à la remise en question de son poste. Ce constat sonne comme un appel à plus de reconnaissance du caractère exigeant et éprouvant du métier.

Si l'on restreint cette observation à la population dont le niveau de stress est dans le rouge (score supérieur à 22), on retrouve le sentiment aigu d'adversité, mais l'on constate également un sentiment d'impuissance devant l'asymétrie du combat et la difficulté de comprendre et traiter les risques cyber. Cette population n'évoque plus le besoin de déconnexion, car elle est engloutie dans l'engagement que requiert le métier. Mais elle se sent démunie face à l'ampleur de la tâche. Le sentiment de découragement est clairement exprimé.

Focus sur les critères générant un avis tranché « Oui, tout à fait » ou « Non, pas du tout ».

Les facteurs les plus contributifs au stress chez les répondants sont les suivants

Top 5 des facteurs les plus contributifs du stress chez tous les répondants	Q
La notion d'adversité qui en fait un métier singulier	Q19
La situation professionnelle est incertaine, une crise majeure peut coûter le poste	Q27
Il faut justifier de l'utilité de ses actions	Q33
Pas de déconnexion, tout le temps sur le qui-vive pour le cas où une attaque surviendrait	Q26
Adaptation et renouvellement permanent dans un contexte de menace très évolutif	Q17

Si l'on se concentre sur les personnes qui sont le plus en souffrance, donc dans la zone rouge, les facteurs les plus marqués deviennent :

Top 5 des facteurs les plus contributifs du stress chez les répondants dont le niveau de stress est dans le rouge (> 22)	Q
La notion d'adversité qui en fait un métier singulier	Q19
La situation professionnelle est incertaine, une crise majeure peut coûter le poste	Q27
Il faut justifier de l'utilité de ses actions	Q33
Sentiment d'impuissance devant l'asymétrie du combat et l'avantage des attaquants	Q22
Difficulté de l'exercice de gestion du risque cyber	Q28

Les 3 premiers facteurs dominants sont similaires pour l'ensemble des répondants et pour la population en zone rouge. Il y a tout de même, chez les répondants dans la zone rouge, en quatrième position, un sentiment d'impuissance face aux attaques. En analysant ce facteur, on constate qu'il est deux fois plus exprimé que pour l'ensemble des répondants. Alors que dans la population générale, le facteur qui arrive en quatrième position exprime plutôt le sentiment de non-déconnexion et d'être tout le temps sur le qui-vive. Par conséquent, si l'on observe le quatrième facteur exprimé, il est donc axé sur le stress de la mise à l'épreuve permanente pour tous les répondants, alors que les répondants de la zone rouge mettent plutôt un sentiment de découragement, donc de peur de l'échec.

À l'inverse les facteurs de stress qui sont les mieux maîtrisés ou les facteurs les plus favorables sont :

Top 5 des facteurs les mieux maîtrisés chez tous les répondants	Q
L'accès à des secrets pouvant être humainement délicats à connaître	Q15
Le fait de ne jamais pouvoir riposter face à une attaque	Q20
Le sentiment d'être personnellement en danger	Q23
Le fait de ne pas connaître son ou ses adversaires dans la plupart des cas	Q25
Le fait d'être soutenu par ses proches pendant la gestion de crises cyber	Q31

Et considérons cette analyse pour ceux qui sont dans la zone rouge.

Top 5 des facteurs les mieux maîtrisés chez les répondants dont le niveau de stress est dans le rouge (> 22)	Q
Le fait de ne jamais pouvoir riposter face à une attaque	Q20
L'accès à des secrets pouvant être humainement délicats à connaître	Q15
Le fait de ne pas connaître son ou ses adversaires dans la plupart des cas	Q25
Le fait d'être soutenu par ses proches pendant la gestion de crises cyber	Q31
Le sentiment d'être personnellement en danger	Q23

Il y a globalement une similitude dans les réponses sur ces 5 facteurs, même si l'ordre des facteurs diffère un peu.

5.3- Zoom sur certains facteurs de stress

Un déficit d'image

38% des répondants, soit 125 personnes déclarent que leur métier souffre « encore » d'un a priori plutôt négatif (Q13). Il aurait bien sûr été intéressant de savoir ce que valait cet indicateur il y a 5 ans. Il est probable que le pourcentage était alors sensiblement plus élevé. Certes le métier est mieux connu et compris aujourd'hui, mais il reste encore un effort important à faire pour le marketing de cette fonction. Il reste à convaincre et à promouvoir, et ce n'est peut-être pas ce que les professionnels de la cybersécurité font le mieux... D'ailleurs 47% se sentent encore incompris, voire parfois jugés excessifs (Q14). Il est important de travailler l'image, un déficit d'image par rapport à son rôle social étant sans doute une source de stress. Il y a quand même eu un tournant important dans la posture prise ces dernières années, qui devrait progressivement améliorer la reconnaissance et le coefficient de compréhension voire de sympathie au sein de l'entreprise. Il faut tout de même poursuivre et accentuer les efforts – et surtout se rendre compte de l'importance de la communication dans ce métier.

Et en dehors de l'entreprise, que répond un enfant à qui l'on demande ce que fait son parent, lorsque celui-ci travaille dans la cybersécurité ? Difficile de prédire si les jeunes enfants voudront faire de la cybersécurité plus tard, au lieu de souhaiter devenir pompier, astronaute ou docteur. Il manque peut-être l'uniforme, la blouse blanche et le stéthoscope autour du cou, la combinaison pour aller dans l'espace ou le casque des pompiers. Difficile de trouver une symbolique matérielle dans un métier qui tourne autour des données et du cyberespace, quoique... Ce terme de « cybersécurité », qui n'a que quelques années, et a succédé à la « Sécurité des Systèmes d'Information », est peut-être une première petite conquête pour améliorer l'image du métier.

Comprendre les compétences requises

Les avis en termes de « hard skills » ne sont pas très tranchés. 60% des répondants pensent posséder l'expertise technique et méthodologique nécessaire (Q16) et seule la moitié d'entre eux estiment avoir la capacité à s'adapter au contexte très évolutif du métier (Q17). Cela signifie tout de même que plus d'une centaine de personnes émettent des doutes sur leur compétences, doutes qui sont certainement sources de stress.

D'où viennent ces interrogations ? Le métier est récent, un certain nombre de répondants ne l'ont pas appris au cours de leurs études. Par ailleurs, le paysage technique dans son ensemble (technologies à protéger, techniques d'attaque, etc.) évolue vite, avec plusieurs grands changements réguliers ; cela ne facilite pas le sentiment de maitrise du sujet. Ce métier est par ailleurs en train de créer ses différentes spécialités, ce qui démontre qu'il n'y a pas un mais plusieurs ensembles de compétences nécessaires. Les repères sont en train de se créer et seront bientôt plus lisibles. Il est probable que la prochaine génération d'experts en cybersécurité aura plus de facilité à se situer, à s'évaluer et à se sentir plus en adéquation avec les compétences attendues.

Vivre l'adversité

82% des répondants confirment devoir affronter des ennemis souvent invisibles (Q19), ce qui en fait certainement une vraie singularité de leur métier. En dehors du secteur de la Défense, il y a peu de métiers en entreprise qui soient dans cette posture de lutte contre des ennemis de l'entreprise ; que ces adversaires soient des individus malveillants ou des organisations criminelles.

Même si 82% des répondants ne se sentent pas personnellement en danger (Q23) ni perturbés de ne pouvoir identifier que rarement la partie adverse (Q25), les professionnels de la cybersécurité sont indéniablement dans une posture intrinsèquement défensive.

28%, soit 91 répondants, sont d'ailleurs plus ou moins découragés devant l'augmentation de la fréquence et de la puissance des cyberattaques (Q21) et autant de répondants sont frustrés de ne pas pouvoir riposter (Q20). Même si ces pourcentages sont minoritaires, ils représentent, en valeur absolue, presqu'une centaine de personnes. La moitié des répondants a un sentiment d'impuissance devant le caractère asymétrique du combat (Q22), ce qui est un indicateur significatif qu'il convient de suivre attentivement.

Le contexte d'adversité est une source bien connue de stress, accentuée par l'intensité de l'agression potentielle et la difficulté d'y faire face. Mais ce contexte peut également créer de l'empathie dans la relation aux employés de l'entreprise, qui peut atténuer ou adoucir la pression perçue. Il peut alors s'opérer une forme de transfert de cette pression en invitant ces employés à contribuer à la défense - la « sécurité est l'affaire de tous ». Les employés de l'entreprise comptent sur l'équipe cybersécurité pour les défendre et cette équipe les invite en retour à être également des acteurs de cette activité de défense.

De la déconnexion et de l'incertitude

La déconnexion est un besoin qui est de plus en plus souvent exprimé dans les entreprises, dans divers secteurs professionnels, et cela a abouti à une loi. Il s'agit de tracer une frontière entre les moments professionnels et la vie personnelle. En réalité les mails ne s'arrêtent jamais le vendredi soir et l'information récente est accessible trop facilement, au bout des doigts, sur son smartphone que l'on fixe plusieurs heures par jour, dans cette obsession générationnelle d'être sûrs de ne rien rater. Certains utilisent le même smartphone pour les échanges pro et perso, ce qui complexifie le travail de tri. Les périodes de confinement et de télétravail ont achevé de brouiller les pistes quant à cette prétendue frontière. En cybersécurité, le métier requiert d'être en permanence à l'écoute de signaux, que ceux-ci expriment un début d'attaque potentielle, chez soi, chez son fournisseur, chez son concurrent, ou qu'il s'agisse de nouvelles failles découvertes dont le score de dangerosité tombe comme un couperet.

Que les signaux soient faibles ou forts, que le feu soit vite éteint ou pas, il existe un sentiment permanent d'incertitude : le fait que tout peut arriver à tout moment et qu'on n'en mesurera que progressivement la gravité. Mais il faut être là, à l'écoute, toujours. Que l'on soit devant un bon match, à dîner chez des amis, sous la douche ou dans les bras de Morphée, l'incertitude est là. 52% des répondants se sentent sur le qui-vive (Q26), sans pouvoir se déconnecter. Même si 78% des répondants peuvent apprécier ce métier fait d'aléas et d'imprévus (Q24), près d'un quart des répondants ne s'y font pas du tout. Le sentiment d'incertitude est cité dans le top 5 des principales causes de stress. Il s'exprime d'ailleurs clairement chez l'ensemble des répondants qui considèrent que leur situation professionnelle est incluse dans cette incertitude intrinsèque au métier. Il ne s'agit donc pas simplement d'être réveillé en pleine nuit pour traiter un évènement sérieux, mais de le faire en considérant que cet évènement risque de vous faire perdre votre poste, si tous les astres ne sont pas correctement alignés ce jour-là. Donc pas de déconnexion pour les métiers de la cybersécurité, une incertitude, une vie de surprises et d'aventures qui peuvent se terminer par une déconnexion définitive et forcée…

Instabilité de la fonction

Ce sujet de limogeage suite à une crise majeure et, plus globalement, celui de l'instabilité du poste peuvent évidemment contribuer au niveau de stress perçu par les responsables Cyber. Cependant la risque de perte de poste en cas

d'incident n'inquiète que partiellement les répondants : 54% estiment qu'une crise majeure pourrait leur coûter leur poste. Ce chiffre monte à 65% si on ne considère que les répondants ayant un niveau de stress élevé (« zone rouge »). On dépasse la majorité mais celle-ci n'est pas écrasante. Ce facteur de stress ne semble pas le plus critique.

Il faut tout de même prendre le temps de se pencher sur cette problématique. Comment se comporte une profession dont plus de la moitié des membres estime qu'ils peuvent « sauter » en cas d'incident ? À l'heure de la surmultiplication des attaques, mais aussi de la généralisation des secteurs touchés, cette majorité peut représenter un risque. On peut se demander si cette peur ne va pas engendrer des comportements discutables, comme le fait de passer sous silence certaines vulnérabilités ou certains incidents, ou comme le fait de consacrer davantage d'énergie à l'attribution des responsabilités plutôt qu'à l'édification de dispositifs de défense solides. Ces éléments d'analyse restent du domaine de l'hypothèse faute de chiffres, mais ils se doivent d'être considérés.

Alors comment améliorer cette situation et éviter des déviances potentielles ? La clé réside dans la perception d'être le fusible d'une crise Cyber. En effet, même si le secteur recrute énormément et fait face à une pénurie de ressources, la perte de son emploi représente une difficulté – dont chacun jugera du niveau de gravité selon sa situation personnelle.

Pour autant, est-ce que chacune des organisations concernées va remercier son RSSI en cas de crise ? Est-ce que cela a été le cas pour les victimes récentes d'attaques médiatisées ? Combien de fois une entreprise peut-elle jouer la carte du fusible, sans se décrédibiliser ? Il est probable que les responsables Cyber surestiment le risque de perdre leur poste, mais cette inquiétude mérite d'être analysée car elle peut avoir des impacts sur les comportements. La question de la reconnaissance, de la confiance dans son poste et dans son management, peut probablement expliquer une certaine distorsion et représente un axe de travail intéressant, notamment parmi la population la plus exposée au stress.

Par ailleurs, il y a une catégorie de professionnels qui reproduit une technique bien connue de la gestion de risques : l'acceptation ! Certains RSSI se déclarent conscients de l'exposition de leur poste et acceptent de vivre avec : « en cas de crise majeure, mon employeur peut décider de se passer de mes services. C'est une des possibilités existantes en réponse à une crise ». Et pour cette catégorie de professionnels, cela ne semble pas constituer pour autant un facteur de stress.

Perception du risque cyber

La gestion du risque Cyber est un exercice difficile pour 62% des répondants. Ce risque est très évolutif, il nécessite d'être souvent réévalué et les stratégies qui permettent de traiter ces risques peuvent connaître des virages rapides et de nombreux changements de priorités.

Il est désormais acquis que l'impact d'une cyber-attaque peut être considérable pour l'entreprise et que la probabilité d'occurrence est significative. Pour autant, si la maturité de l'entreprise progresse en matière de cybersécurité, l'information et les systèmes à protéger ont des contours de plus en plus flous. L'exercice de focalisation est ardu, d'autant qu'il faut souvent refocaliser pour prendre en compte le caractère très changeant de ce risque.

Gérer les crises

La gestion de crises Cyber est un exercice relativement récent. Même s'il existe aujourd'hui une littérature relativement abondante et un certain nombre de formations dans ce domaine, il y a peu de références en la matière, peu d'exemples de scénarios permettant de construire des modèles

de réponses. Un certain nombre d'histoires sont gardées confidentielles, ce qui rend difficile la modélisation.

Pour autant, il apparait que la pression liée à la gestion de crise Cyber est soit bien, soit plutôt bien vécue par près de 84% des répondants (Q29). Score réconfortant même s'il ne faut pas négliger la cinquantaine de professionnels qui subissent et affectionnent peu l'exercice.

Cette gestion de crise s'exerce dans des bonnes conditions personnelles puisque 81% des répondants se déclarent soutenus par leurs proches (Q31).

Finalement, l'absence de référence sur la conduite de crises Cyber est peut-être un avantage, car cela permet d'éviter des biais d'ancrage sur une pratique ou des scénarios qui ont bien fonctionné dans le passé, mais ne serait pas adaptés aux menaces actuelles.

L'AFPA et les risques psychosociaux

L'AFPA a mené une étude sur le métier très récent de DPO, et s'était intéressée aux risques psychosociaux pour cette profession. L'étude AFPA rappelle que les facteurs de risques psychosociaux peuvent se décliner en 5 axes d'analyse :

1. L'intensité et le temps de travail
2. Les exigences émotionnelles
3. L'autonomie et les marges de manœuvre
4. Les conflits de valeurs
5. L'insécurité de la situation de travail

Si l'on met en regard les questions posées lors de l'enquête CESIN-Advens par rapport à cette typologie de risques psychosociaux, on constate, par exemple, que :

→ Le type de facteur n°1 peut s'appliquer notamment à la complexité du travail et à la gestion des urgences et des crises (Q29 à Q31). Ce risque existe clairement dans la Cyber, il est même jugé élevé.

→ Le n°2 représente généralement la relation aux tiers : il faudrait voir dans quelle mesure la situation d'adversité peut être assimilée à cet axe (Q19), mais il ne semble pas que cette relation aux tiers soit un risque jugé élevé par les répondants.

→ Le n°3 représente les risques de monotonie et de manque de marge de manœuvre : cet axe est assez éloigné des risques évoqués en cybersécurité, où à l'inverse, la variabilité et l'évolutivité des activités sont grandes (Q17), a minima pour les Responsables Cyber. Ce risque peut a contrario concerner certains métiers de la cyber, comme les analystes de SOC, par exemple, mais ceux-ci n'ont pas été intégrés dans le panel des personnes interrogées. On parle alors de cyber-fatigue et la promesse de certaines solutions de sécurité est de remplacer les tâches susceptibles de provoquer ce type de fatigue et d'usure par des systèmes automatiques plus rapides que les humains.

→ Le n°4 concerne des potentiels conflits de valeurs éthiques : ce point est abordé dans les questions Q15 et Q20 par exemple. Il semble que les Responsables Cyber soient à l'aise avec les questions éthiques formulées dans l'enquête. Celle, par exemple, concernant la détention des secrets de salariés. Il pourrait être intéressant d'étendre ces questions éthiques à d'autres cas, lors de futures enquêtes : par exemple, les cas de malveillance interne qui sont toujours délicats à traiter, les demandes de rançon par des acteurs malveillants qui posent la question du financement ou non de la cybercriminalité, les cas d'attaques sur fond de militantisme pour des causes pouvant créer de l'empathie chez le Responsable Cyber, etc.

→ Le n°5 renvoie à la question Q27 relative à la crainte de perdre son emploi, mais aussi aux questions Q33 et Q34 sur l'utilité de son action et sa responsabilité personnelle.

6

Une prise de conscience
Réactions face aux résultats

6.1- Le regard du Coach

Yann OFANOWSKI

Spécialiste des Ressources Humaines, de la gestion des talents et du management, est désormais coach, avec une spécialisation en matière de résilience émotionnelle. Son analyse des résultats du PSS10 a permis de commencer à travailler sur les pistes de solutions.

« Les résultats sont préoccupants. Un grand nombre de réponses (28%) se situe en zone rouge, parfois avec des niveaux d'intensité de stress très élevés comme les 7% de participants qui présentent un score supérieur à 28.

Quelques considérations sont à prendre en compte dans l'interprétation de ces résultats :

→ Les stress importants (>22) sont gérables ponctuellement. Un risque pour la santé se pose lorsque ces niveaux de stress perdurent et s'installent pendant plusieurs mois, voire plusieurs années d'affilée. La PSS10 prend une « photo » du stress perçu les 30 derniers jours. Il serait intéressant de prendre d'autres « photos » et de mettre les clichés bout à bout à l'avenir.

→ L'enquête a eu lieu en pleine période de pandémie. Nous savons que les effets psychologiques liés à cette période ont été délétères (confinement, surcompensation de travail à la maison, réduction d'activités physique, coupure du lien social, maladie, vulnérabilité des proches etc.). Nous ne pouvons malheureusement pas comparer ces résultats à d'autres professions (manque de données) mais on peut s'attendre à ce que l'impact soit également important dans d'autres secteurs.

→ Les directeurs Cybersécurité et RSSI sont des cadres dirigeants, ce niveau de responsabilité est sans doute davantage soumis au stress que la moyenne des « cadres/ingénieurs ». Là encore, nous n'avons pas les données permettant une segmentation plus fine.

→ Même si la composante de stress spécifiquement liée à la nature du leadership Sécurité SI reste difficile à isoler, ces résultats sont un appel à l'action et à la prévention, au moins pour la partie de la population concernée.

Une partie de la population a besoin d'aide. Les verbatim et témoi-

gnages nous apportent un éclairage sensible sur certaines racines de ce stress. Il me semble illusoire de vouloir faire évoluer les stresseurs externes, c'est-à-dire les éléments culturels, managériaux, humains, techniques ou financiers impactant les RSSI. Ces derniers font partie d'un système sous tension, parfois asservissant, dans une société en accélération constante et de plus en plus dépendante de la connexion virtuelle. L'enjeu prioritaire - et à notre portée - n'est pas de changer ce système (trop compliqué) mais d'apprendre aux individus à s'en protéger et à y naviguer plus sereinement. »

6.2- Le regard du Soignant

Alain LIVARTOWSKI

Le Docteur Alain Livartowski, oncologue à l'Institut Curie, considère que le sondage réalisé est particulièrement éclairant pour quelqu'un qui n'est pas de la profession, et nous livre sa réaction.

« Les remarques qui suivent sont celles d'un médecin dont le devoir est d'être attentif aux risques professionnels qui peuvent avoir des conséquences sur la santé, psychique en premier, mais occasionner aussi des désordres somatiques.

Les métiers de RSSI ou de Directeur cybersécurité sont considérés par les intéressés comme nécessitant des compétences techniques qui évoluent sans cesse. Ils ressentent les responsabilités qui leur incombent avec des difficultés qui s'accumulent et un nombre de tâches à assumer qui vont grandissantes. Sur le plan des compétences, ils se disent en capacité à gérer les risques les contrôler, les maîtriser.

Cette responsabilité importante associée à une compétence technique forte devrait être la garantie d'être reconnus par les autres ; pourtant, ils ne se sentent pas suffisamment reconnus ou soutenus par les collègues (38 % le pensent) ou leur hiérarchie : une majorité (54 %) pensent qu'en cas de crise majeure, cela peut leur coûter leurs postes.

Pour beaucoup, ceci peut occasionner nervosité, stress (54 % souvent et assez souvent) auxquels il faut ajouter les 31 % qui le ressentent parfois. Ainsi, seulement 15 % y échappent.

La difficulté du métier, les responsabilités, l'évolution constante des risques sont cités comme étant à l'origine de ce stress. Une des raisons est que les risques sont difficiles à prévoir et peuvent devenir rapidement sérieux avec des conséquences graves.

La première conclusion est, qu'en tant que médecin, j'observe que le pourcentage de personnes en situation de stress est élevé, avec pour certain probablement une souffrance et l'entrée en « zone rouge ». Cette question ne peut pas être occultée et une prise de conscience est nécessaire. Un des moyens de l'éviter est déjà de le reconnaître et de les soutenir dans l'entreprise.

La deuxième conclusion est celle d'un médecin cancérologue, confronté à des maladies graves, des décisions difficiles et maniant des traitements qui peuvent s'avérer dangereux pour le patient. Les cancérologues également sont soumis au stress. Ce qui sauvent les cancérologues du « burn out », c'est la reconnaissance du travail, le soutien entre équipes médicales mais aussi administratives et des supérieurs hiérarchiques. Ce sont les mêmes remèdes qui peuvent permettre d'éviter le stress de ceux qui ont pour mission de protéger les systèmes d'information des entreprises et au-delà les entreprises elles-mêmes. »

6.3- Le regard de la Directrice Cybersécurité

Mylène JAROSSAY

Directrice Cybersécurité du Groupe LVMH et présidente cofondatrice du CESIN, nous livre son analyse.

« Cette enquête a tenu toutes ses promesses de nous éclairer sur la charge mentale des professionnels de la cybersécurité. Merci aux membres du CESIN d'avoir répondu en nombre à cette enquête, car leur implication a permis d'obtenir des résultats vraiment exploitables. Et même si les résultats de l'enquête sont très préoccupants, l'enquête est riche en enseignements. Cela nous motive à poursuivre et étendre la démarche. Approfondir l'analyse, mais aussi, dès à présent, engager un ensemble d'actions pour identifier et mettre en œuvre des pistes d'amélioration. Car on ne peut pas rester devant les constats de l'enquête sans chercher à comprendre et traiter la problématique qui en est ressortie.

L'intensité du stress, évaluée dans la première série de questions, est clairement élevée, et le nombre de personnes en souffrance, dans la zone dite « rouge » est important. Quant aux causes de ce stress, les questions proposées ont permis de livrer quelques clés de lecture. La compréhension de ces causes peut se faire en deux temps. D'abord, en considérant les grands ratios, question par question. En faisant cela et en première intention, il semble alors que ça ne va pas si mal. Mais si on examine de près les résultats avec une logique de profilage, en partant de quelques combinaisons de critères, appliquée à la population des répondants, on saisit mieux les conclusions inquiétantes sur le niveau de stress, car on voit apparaître un certain nombre de profils en réelle difficulté sur plusieurs axes clés du métier.

Finalement l'ensemble des questions de l'enquête est une invitation à élaborer des pistes d'interprétation plus poussées mais aussi à rechercher des solutions.

Il est sans doute judicieux, par exemple, de classer les causes de ce stress en cernant celles qui paraissent conjoncturelles ou temporaires, et en concentrant sa recherche de pistes d'amélioration surtout sur celles qui risquent de se pérenniser, car intrinsèquement et intimement liées au métier cible. Les facteurs qui devraient naturellement perdre de leur influence sont principalement dus au temps nécessaire à l'installation du métier. Notre profession est encore récente. Il faut finir de spécifier, déployer et faire connaître, dans l'entreprise, les spécialités et l'organisation qui la constituent. Cela permettra aux professionnels de la cybersécurité, de mieux intégrer et promouvoir leurs missions et d'avoir des repères pour se situer, pour trouver leur place, dans et hors de l'entreprise. Le second élément, en partie lié au premier, est une meilleure compréhension par le top management, du rôle que doivent jouer ces professionnels pour mettre en œuvre des solutions et des services, mais aussi pour instiller la cybersécurité partout dans l'entreprise, partout où se trouve de l'information à protéger. Avec l'augmentation des menaces et de la sinistralité, la prise de conscience est en train de se faire. Mais à en juger par le taux de répondants qui craignent pour leur poste, la maturité n'est pas toujours là. Elle arrivera forcément bientôt, et peut-être de façon brutale, par la force des incidents.

Il faudrait également questionner et préciser les impacts dans le quotidien de ces niveaux de stress, impacts sur le travail fourni, sur la performance, et impacts sur la vie sociale et familiale. Il faudrait sans doute creuser davantage les activités qui semblent les plus difficiles et éprouvantes à gérer pour les répondants. Il pourrait aussi être intéressant de mesurer la perception du métier au sein des entreprises, afin d'estimer l'écart entre l'image que les Responsables Cyber pensent avoir et ce qu'en pensent vraiment leurs collègues. Il serait sans doute utile également de nuancer les réponses sur les situations de stress par rapport à l'âge, l'ancienneté dans la profession, les études faites et le parcours professionnel. Un complément d'étude pourrait intégrer des questions relatives aux compétences, notamment sur les soft skills requises pour mieux appréhender voire conjurer le stress provoqué par la fonction.

Enfin, un approfondissement serait bienvenu pour confirmer que les métiers de la cybersécurité ne sont pas soumis à trop de conflits intérieurs en matière d'éthique et de valeurs.

En résumé, il y a largement matière à explorer davantage. Mais cette exploration devrait s'inscrire dans une démarche de suivi plus long terme, pour observer des tendances. L'idée est de fixer un cadre d'indicateurs permettant d'observer chaque année l'évolution du stress et des facteurs clés qui l'aggravent, ou au contraire peuvent le rendre positif. Ceci afin d'observer comment ce stress évolue au fil des ans, car il y a des transformations importantes du métier en ce moment, la population qui l'exerce est en forte croissance, et ce serait précieux d'observer comment se fait cette transformation par rapport au vécu des professionnels.

Cette étude ouvre un éventail d'interrogations. Est-ce que la reconnaissance est une clé dans la réduction du stress ? Est-ce que ce stress nuit ou est un atout à la performance ? Ou comment peut-on agir pour convertir ce stress en atout pour la performance donc aussi pour la réduction du stress ? Ou après tout, peut-on exercer correctement cette fonction sans stress ? Ce métier est-il définitivement un métier de sprinters plutôt qu'un métier de marathoniens ?

Et si les éléments qui paraissent des sources de stress étaient aussi des opportunités ? En effet, on parle de stress positif ou stimulant. Disons-le, la cybersécurité est un métier pour qui aime l'aventure, un métier pour les Indiana Jones du numérique, qui ne dorment que d'une oreille. C'est un métier de suspense, où l'on ne s'ennuie jamais, qui se déroule en plusieurs épisodes, plus intenses que n'importe quelle fiction. C'est un métier de vitesse sur terrain accidenté, avec des instruments de navigation parfois indisponibles. C'est aussi un métier de stratégie qui joue et compose avec des multiples facteurs techniques, humains, contractuels. Un métier qui doit prendre du recul et construire, tout en considérant l'immédiateté. Un métier qui baigne dans l'innovation pour gagner ces matchs contre des acteurs malveillants toujours plus performants. C'est un jeu du chat et de la souris, donc un jeu ? C'est un métier global car il s'agit de transformer des pratiques, de s'insinuer dans le quotidien de tous les acteurs de l'entreprise. C'est un métier de sagesse qui devrait accompagner le numérique dans une « logique de quick and

secure ». C'est un métier gratifiant, comme tout métier du soin, car il s'agit de protéger l'outil de l'entreprise. C'est un métier d'humilité, car on ne gagne pas à tous les coups. Et c'est un métier d'ambition car la tâche est incroyablement complexe.

Avec tous ces superlatifs, on devrait sans doute parvenir à emmener les professionnels de la cybersécurité, non vers une disparition du stress, mais vers une sublimation des aspects stressants du métier. »

6.4- Le regard du Fournisseur de Services Cyber

Benjamin LEROUX

Directeur Marketing et RSSI de la société Advens, nous partage son regard sur l'étude.

« Lorsque j'ai proposé ce thème d'étude au CESIN, je ne savais pas vraiment où tout cela mènerait. Les articles lus dans des médias américains ou anglais m'avaient mis la puce à l'oreille, tout en craignant un traitement un peu racoleur du sujet, dans l'espoir de faire du clic !

L'accueil du CESIN a été des plus positifs et des plus motivants. Faire appel à cette communauté allait permettre de s'appuyer sur un nombre important de responsables Cyber, et disposer ainsi de chiffres et de statistiques crédibles et réalistes. L'objectif était avant tout de se faire une idée de la situation. La question du stress d'une population exposée à des incidents et des crises peut sembler rhétorique ! Qui ne serait pas stressé face à cette menace Cyber dont on dit tous les jours qu'elle croit sans limite ? Il nous a tout de même semblé pertinent de creuser et d'essayer d'en savoir plus.

La démarche d'étude était particulièrement importante. Outre le recours à une enquête, en espérant toucher le plus grand nombre de RSSI, il fallait également un regard neutre, et idéalement d'expert, sur ces sujets du stress et de la santé mentale. Notre expertise commune, au CESIN et chez Advens, ne couvre pas spécialement ces problématiques. Il fallait donc avancer avec prudence ou être guidé par des spécialistes, ce qui a pu être fait grâce aux intervenants externes qui ont contribué.

Ces différents ingrédients ont permis une mesure du niveau de stress ressenti et une première recherche de causes, pour celles relatives à la nature du métier. Le niveau moyen est préoccupant, avec certains groupes flirtant avec une limite inquiétante.

Il est intéressant de noter que cette analyse s'est faite en deux temps. Les intervenants issus du monde de la Cyber ont vu le « verre à moitié plein », et se sont réjoui que près de 40% des répondants allaient bien ! Et très vite les experts ont alerté sur cette erreur de diagnostic : 60% de profils exposés à un stress à risque, c'est beaucoup, et même beaucoup trop. Le recours à l'échelle PSS a permis une mise en perspective et a mis en lumière cette situation préoccupante. Il y avait donc bel et bien matière à étudier…

L'étude des facteurs générateurs de stress s'est révélée tout aussi intéressante pour amorcer la suite des travaux : la recherche de solutions pour maitriser voire réduire ce stress. Là aussi la méthode peut faire débat et doit être cadrée avec soin. Le stress peut découler d'une situation personnelle, dont on sait que la pandémie en a complexifié plus d'une. Il peut aussi être lié à l'employeur, au management, aux relations interpersonnelles au travail. Tous ces facteurs sont importants mais dépassent le cadre de la Cyber… et il aurait été trop complexe de s'y aventurer.

Il apparait alors que plusieurs composantes du métier de RSSI sont génératrices de stress. Si l'on écarte les facteurs externes, sur lesquels il est difficile d'influer (comme par exemple le caractère aléatoire d'une attaque ou le contexte d'adversité de la lutte contre la menace) il reste de nombreux facteurs comme la responsabilité, la difficulté à déconnecter, la crainte de sauter ou encore la complexité de la fonction sur lesquels on peut, et on doit, travailler.

Il faut désormais prendre le temps d'analyser ces premières conclusions pour définir les actions les plus pertinentes. On identifie aisément un ensemble d'actions visant à faire parler du sujet, à oser l'aborder. Et très vite on pense à des actions pour réduire le niveau de stress, notamment en expliquant encore mieux le métier, ses particularités et ses dépendances avec les autres métiers de l'entreprise. Cette approche pédagogique devrait permettre une meilleure reconnaissance du rôle, et au passage devrait contribuer à une meilleure compréhension du risque Cyber. On voit déjà un premier résultat « win win ». D'une part, le RSSI améliore sa reconnaissance et la compréhension de ses actions, et pourra bénéficier du soutien des autres acteurs de l'entreprise. D'autre part, les collaborateurs sont mieux armés pour comprendre la menace et potentiellement réduire les comportements à risque.

Ce premier exemple illustre pleinement l'ambition de la prochaine étape de nos travaux. Identifier des chantiers permettant, d'une part, de réduire le niveau de stress ou de le contenir dans un état de stress positif et stimulant et, d'autre part, de renforcer l'efficacité des dispositifs de Cybersécurité, via notamment une meilleure intégration dans les métiers de l'entreprise et une approche plus positive et préventive. »

7

Approfondir et observer

L'enquête a ouvert un champ d'interrogations sur la charge mentale pour les métiers de la Cyber. Mais une seule enquête n'est pas suffisante pour mener une action long terme de prévention et de traitement des risques psychosociaux pour cette profession.

Il est important d'approfondir certains sujets, de confirmer des hypothèses faites lors de cette enquête, et surtout de mesurer dans le temps l'évolution de ce stress. En comprenant l'origine du stress et l'évolution de la situation des Responsables Cyber dans l'entreprise, on devrait pouvoir accompagner au mieux cette évolution et tenter d'apporter une aide concrète aux professionnels.

Il est donc proposé de mettre en place une observation annuelle du stress, en suivant dans le temps quelques indicateurs clés. Il est également envisagé de compléter l'enquête actuelle en approfondissant certaines thématiques.

Pour cela, il est proposé d'organiser quelques débats au sein de la communauté CESIN, afin de construire ensemble ces indicateurs et cette démarche d'approfondissement.

8

Des paroles aux actes
Premières réflexions sur les solutions

8.1- Que faire ?

L'étude n'avait pas pour objectif de travailler sur les solutions de gestion du stress. Comme introduit précédemment, elle visait à se faire une conviction sur le problème et sur ses origines. Les résultats sont sans appel. Les professionnels et professionnelles de la Cybersécurité font en majorité face à un stress aux effets négatifs. Et certaines caractéristiques intrinsèques à leur métier contribuent à ce niveau de stress potentiellement dangereux.

Une fois ce constat établi, et démontré par les chiffres, il est difficile d'en rester là ! D'une part parce que ça n'est pas dans les habitudes des initiateurs de l'étude, ni des spécialistes qui y ont contribué. Et d'autre part parce que la situation est risquée. Comment protéger correctement une entreprise et son environnement numérique si on ne se sent pas protégé soi-même ? La profession peut-elle se trouver grandie par un travail sur le stress et ses causes ? Comment nous aider et aider la communauté, sinon la société ?

L'importance de la Cybersécurité n'est plus à démontrer. L'importance de « sécuriser » les Femmes et les Hommes qui l'orchestrent jour après jour doit, à son tour, être indiscutable. Ceci étant dit, que faire pour travailler sur ce sujet, à la fois nouveau pour les experts Cyber mais de mieux en mieux appréhendé par les spécialistes de la santé mentale puis par extension des ressources humaines, du management, etc. ?

Avec l'aide des intervenants externes, et au fil des différentes prises de recul, certaines solutions apparaissent dès à présent. Les voici abordées ci-dessous, selon qu'elles se concentrent sur les pratiques de professionnels concernés ou qu'elles portent sur les écosystèmes organisationnels, académiques voire sociaux.

Ces propositions ont pour objectifs, soit de traiter les conséquences de ce stress, soit de s'attaquer aux causes du stress en identifiant des actions susceptibles de les réduire.

8.2- Au sein des communautés

Au sein des communautés, avec en tête l'exemple de ce que fait une association comme le CESIN, un certain nombre de solutions peuvent découler des pratiques utilisées pour traiter le stress en entreprise, à l'échelle globale ou à l'échelle de certaines professions ou profils de professions – comme les cadres ou les dirigeants par exemple.

L'objectif de ces actions est double. Le premier volet vise à

poursuivre la prise de conscience et la reconnaissance de la problématique. Le second vise à travailler sur des pratiques visant à réduire le stress. A ce stade des réflexions, trois pistes sont proposées et seront travaillées par Advens et par le CESIN.

Idée 1 : Webinaires « Résilience face au stress »

L'outil du webinaire a été largement utilisé, pour ne pas dire usé, pendant les derniers mois, en particulier ceux de confinement. Il est désormais maitrisé par tous et peut être utilisé pour ce sujet encore neuf.

Il s'agit donc d'utiliser ce format de façon régulière pour proposer un espace d'échange et de travail collectif, et ainsi impulser une large dynamique collective au sein de la profession. Le thème d'ensemble pourrait être le « Care ». Cet anglicisme provient du mot anglais signifiant « prendre soin ». Il vise à désigner sous un mot clé les différentes méthodes, dispositifs et réponses que l'on peut apporter aux situations de vulnérabilité personnelle des responsables Cyber.

Le contenu de tels webinars est à construire mais peut s'appuyer notamment sur l'apport de théorie et de savoir, le partage de cas pratiques, les retours d'expérience. Comme pour cette étude, l'intervention de spécialistes sera bénéfique pour en assurer la qualité et l'efficacité.

Seront, par exemple, à considérer les thématiques suivantes :

→ Changer de posture face au stress (neurosciences) dans un contexte de menace Cyber en pleine explosion,

→ Mettre son corps au service de son mental (embodiment),

→ Trouver le bon niveau de tension (adaptive leadership) pour le niveau de maturité Cyber de son organisation,

→ Faire face au « trop » (surinvestissement et addictions comportementales),

→ Naviguer dans la complexité (immunity to change),

→ Etc.

Idée 2 : Ateliers d'approfondissement

L'approfondissement vise à travailler en groupes plus réduits (de 8 à 10 participants), dans la durée et par exemple dans une dynamique inter-entreprise. Chaque groupe est constitué pour six mois. Durant cette période, les participants se soutiennent mutuellement dans leur acquisition de compétences (cognitives, émotionnelles et comportementales). L'objectif pour chacun est de renforcer sa posture individuelle face au stress et de gagner en agilité émotionnelle.

Il existe un fossé entre l'évolution des sciences cognitives et comportementales depuis deux décennies et leur application concrète par la majorité d'entre nous. Ce type d'ateliers peut apporter des solutions très concrètes pour les participants, sur des sujets qui sont souvent négligés voire inconnus.

C'est ainsi que chacun pourra grandir et se renforcer face au stress. En effet, l'intelligence collective mise au service du renforcement individuel a largement démontré son efficacité (codev, groupe de parole, sociodrame etc.).

Des ateliers en petits groupes ont pu être menés à distance depuis le début de l'année 2020, sur d'autres thématiques, pour s'adapter à la situation sanitaire. Ce sont des dispositifs relativement simples à mettre en place et accessibles par les participants.

Idée 3 : Séminaire

La piste est à considérer une fois la situation pandémique stabilisée. Cependant il s'agirait d'organiser une journée complète de conférences et d'échanges sur la problématique du stress dans les métiers de la Cybersécurité. Elle viserait à renforcer la prise de conscience de la profession.

Elle pourrait aussi s'ouvrir à d'autres acteurs, comme notamment les supérieurs hiérarchiques des responsables Cyber (DSI, DAF, Secrétaires Généraux, DGA, etc.) – ceci dans une logique de sensibilisation et d'intégration de ces populations aux réflexions et aux travaux de gestion du stress.

Idée 4 : Portraits de Responsables Cyber

Cette piste a déjà été envisagée par le CESIN, en amont de cette étude sur le stress. Il s'agit d'établir les portraits de membres du Club. Aujourd'hui la cybersécurité est décrite à travers un ensemble d'activités et de pratiques. Il s'agit de compléter cette vision du métier en apportant les vécus des personnes qui l'exercent au quotidien, dans sa globalité et dans toute sa complexité et sa subtilité. Il sera ainsi proposé aux membres du CESIN qui le souhaitent de transmettre ce qu'est et ce que représente ce métier pour eux, dans ses ambitions, dans ses doutes et dans ses épreuves. Ces portraits individuels, en complément de l'enquête statistique globale, apporteront certainement l'éclairage des small data, que les cliniciens et chercheurs affectionnent, pour identifier des situations et scénarios atypiques et intéressants que les moyennes sont susceptibles de gommer. Bien sûr, ils ne seront pas seulement axés sur le stress, mais cette dimension sera forcément présente.

8.3- Dans le parcours professionnel

Au-delà des cercles professionnels réunissant les responsables

Cyber, le champ des possibles est bien plus vaste. Le sujet de la gestion du stress a été largement traité par d'autres professions, et ce via de nombreux dispositifs et outils. Les pistes proposées à ce stade ne sont que ponctuelles et ne garantissent aucune exhaustivité ! Elles visent à ouvrir les réflexions pour un maximum de créativité mais aussi d'efficacité dans les solutions, en réaction comme en prévention.

Idée 1 : Dès la fiche de poste

Aujourd'hui les fiches de postes intègrent assez peu la question du stress. Il pourrait y avoir un certain nombre d'éléments dans les fiches de poste qui nomment et adressent clairement les causes potentielles du stress telles qu'elles sont apparues dans l'enquête. La communauté CESIN pourrait travailler sur exemples de fiches de poste, qui prenne en compte les enseignements de l'enquête, soit pour informer et faire reconnaître l'exigence du métier au plan de la charge mentale, soit pour intégrer ces éléments dans le descriptif des activités. Par exemple, il semble utile de rappeler, dans la fiche de poste, le caractère connecté du poste, le fait que ce poste conduit à prendre des actions utiles, parfois contraignantes, et qui n'empêcheront pas tous les scénarios mais limiteront les risques. Il faudrait aussi rappeler le caractère évolutif qui demande une adaptation permanente et intégrer la veille et l'adaptation aux évolutions comme une activité à part entière du métier et non comme un élément à subir.

Idée 2 : Intégration au parcours de formation

La première des choses à faire peut sembler évidente : il s'agit de s'appuyer sur l'employeur et son département RH pour aider le RSSI à renforcer ses compétences en matière de résistance face aux facteurs de stress. De nombreux catalogues de formation en entreprise intègrent désormais ces problématiques.

Cela peut passer tout simplement par l'intégration du RSSI dans le bon parcours de formation déjà existant. Compte-tenu du caractère parfois « normé » de ces éléments, cela peut passer par une évolution du statut du RSSI, pour le faire entrer dans une population (au sens RH) plus proche des métiers de direction, de prise de décision et d'impact global au niveau de la structure.

On peut imaginer que pour les directeurs Cyber, le passage au statut de cadre-dirigeant peut s'accompagner dans certaines structures de cette mise à disposition de formation tournée autour du stress, du développement personnel et du leadership.

Pour les structures les moins matures, c'est une occasion pour les

responsables formation de se doter de contenus et de formation adaptées à cette problématique qui dépasse le strict cadre de la Cyber.

Idée 3 : Reconnaissance et soutien dans l'entreprise

La seconde piste concerne la reconnaissance et le soutien des professionnels de la Cybersécurité par leurs collègues et par les autres professionnels au sein de leur organisation. Cette approche est issue des mécanismes mis en place dans le monde la Santé.

Si l'objectif est simple à exprimer, les dispositifs pour l'atteindre sont plus complexes. Ils peuvent changer du tout au tout selon l'organisation concernée, sa culture et ses modalités internes. Il s'agit d'expliquer et de valoriser les travaux des équipes Cyber de manière à faire reconnaitre leurs particularités ainsi que leurs apports à l'organisation.

Cela peut passer par des actions de « marketing » interne, de communication mais aussi, plus simplement, par des moments de dialogue entre le Responsable Cyber et homologues au sein d'autres métiers de l'organisation.

Idée 4 : Sensibilisation orientée Action

La quatrième piste est liée à la précédente dans sa finalité : la reconnaissance et le soutien. Il s'agit de faire en sorte que le plus grand nombre de collaborateurs de l'organisation protégée par le Responsable Cyber soient conscients des particularités de ce métier et des difficultés potentielles. Il s'agit donc de développer de l'empathie vis-à-vis de l'équipe Cyber.

Cela peut avoir un double niveau de retombées. En premier lieu, l'organisation va globalement prendre conscience du stress potentiel de son responsable Cyber et devrait avoir un mouvement naturel de soutien et de reconnaissance. En second lieu, cela augmentera le niveau global de sensibilisation à la cybersécurité, via une meilleure compréhension de ses enjeux, et donc renforcera le niveau de protection de l'organisation.

On retombe ainsi sur les objectifs de la sensibilisation des collaborateurs. Cependant, pour atteindre le double niveau d'objectifs, il convient de mener la sensibilisation de façon à faire prendre conscience des risques certes mais aussi et surtout des postures, dispositifs et actions à mettre en place pour maitriser ces risques. Cette sensibilisation « orientée Action » doit embarquer les personnes ciblées pour les mettre à la place des professionnels de la Cybersécurité le temps d'une action de sensibilisation…. Mais aussi et surtout leur donner les moyens d'agir pour faire face durablement et efficacement aux

menaces jouant sur l'Humain. On peut imaginer des actions sous forme d'immersion dans le quotidien des équipes de sécurité opérationnelle ou des jeux de rôle par exemple. La diffusion de contenus pédagogues et accessibles à tous, expliquant les mécanismes de l'attaque et de la défense, peut également être bénéfique.

On peut s'attendre alors à un cercle vertueux : le renforcement de la défense par les collaborateurs va réduire le niveau de risque et le nombre de crises… et devrait ainsi permettre une meilleure régulation de la charge mentale des équipes Cyber !

Idée 5 : Apprentissage et participation du monde académique

La dernière piste vise à travailler le problème bien plus en amont, dans une logique de prévention. Il s'agit d'intégrer un volet sur le stress et la résilience émotionnelle aux différents cursus de formation à la Cybersécurité.

Le monde académique accueille de façon encore assez récente le sujet de la Cyber. On sait que de nombreux Responsables Cyber en poste ont appris sur le terrain, faute de formation disponible. On sait également que les formations actuelles sont parfois incomplètes, car proposées sous forme de complément ou de spécialisation lors d'une formation en informatique par exemple. Cependant la dynamique globale s'améliore et les formations sont de plus en plus nombreuses.

Il est donc temps d'intégrer à ces cursus de formation des modules sur l'Humain, et en particulier sur l'Humain responsable de la cybersécurité. Cela peut passer par plusieurs cours, ateliers ou activités sur le développement personnel, le suivi de sa santé mentale, le partage sur les particularités de la Cybersécurité pouvant impacter tout cela. Là-encore, le sujet a déjà été traité et des contenus existants dans d'autres formations doivent pouvoir être exploités pour les contextualiser au sujet.

9

Conclusion

L'Humain, toujours et encore

Cette étude a été lancée sur la base d'un questionnement simple : les Responsables Cybersécurité en France, qu'ils soient RSSI, Directeurs / Directrices Cyber ou autres, sont-ils soumis à un niveau de stress particulièrement élevé ? Le questionnaire rempli par 330 professionnels a permis d'apporter une réponse. L'analyse de ces résultats, avec le concours de spécialistes, a permis de comprendre le niveau de gravité de la situation mais aussi d'identifier quelques-unes des causes de ce stress dans les composantes-mêmes du métier.

Oui, les RSSI sont soumis à un stress. Ils sont 61% à ressentir un stress dont les effets peuvent être négatifs. Ils sont 28% à faire face à un stress de niveau élevé dont les conséquences peuvent être nuisibles sur la santé.

Oui, le métier contribue à ce stress. C'est un métier marqué par l'adversité, marqué par une situation de lutte incessante contre un ennemi souvent invisible, avantagé dans ses moyens d'attaquant, ou a minima bénéficiant de l'effet de surprise ou de l'asymétrie qui fait qu'il suffit à l'attaquant de trouver une seule porte laissée ouverte, tandis que le défenseur doit veiller à ce que toutes les portes restent bien fermées. C'est un poste éprouvant au sens strict du terme, car soumis à des épreuves. Il est fragile, car la reconnaissance n'est pas systématiquement alignée avec l'importance des enjeux de la cybersécurité pour l'organisation à protéger.

Il faut donc utiliser les résultats de ces travaux pour améliorer la situation, améliorer le quotidien de celles et ceux qui protègent chaque jour la vie numérique des entreprises. C'est une obligation pour que chacun de ces professionnelles et professionnels vive mieux son métier et s'épanouisse. Au-delà du développement personnel, c'est également la clé d'une réussite professionnelle. Mieux gérer son stress c'est aussi s'aider à être plus performant, à faire face à l'aléa et aux crises avec davantage de sérénité, tout en protégeant son espace et son temps personnel, c'est-à-dire en gérant le subtil équilibre entre vie professionnelle et vie personnelle, de plus en plus mêlées. Cette amélioration passera notamment par une meilleure explication et meilleure valorisation des travaux des RSSI et des directeurs et directrices Cyber. Le marketing du rôle, sujet souvent abordé, doit être amélioré. Expliquer les caractéristiques du métier, valoriser la diversité des problématiques, démystifier les modes opératoires des attaquants, préciser ce que chacun dans l'organisation peut apporter : autant d'actions qui peuvent améliorer la reconnaissance et accroitre le soutien que sont en droit d'attendre les professionnels de la Cybersécurité.

Grâce à des professionnels de la Cybersécurité plus performants, c'est toute la Cybersécurité qui deviendra plus performante. Les entreprises et les organisations publiques seront mieux protégées, seront plus efficaces pour se concentrer sur les défis qui leur sont propres.

Le facteur humain a souvent été étudié dans la Cybersécurité, car considéré soit comme un facteur récurrent de failles et d'incidents, soit plus récemment, de façon plus positive, comme une source de contribution à la cyberdéfense. Les programmes de sensibilisation sont légion, chacun apportant son contexte professionnel, ses souhaits d'innovation ou son propre vécu. Malheureusement d'autres humains ont sans doute été négligés : celles et ceux qui font la Cybersécurité. Il est temps de s'en préoccuper, pour en améliorer le quotidien et contribuer à une société numérique plus sûre et plus équilibrée.

10

Annexes
Questionnaire et données d'étude

10.1- Annexe 1 – Questionnaire détaillé

Comme présenté dans le document le questionnaire d'étude est composé de deux parties.

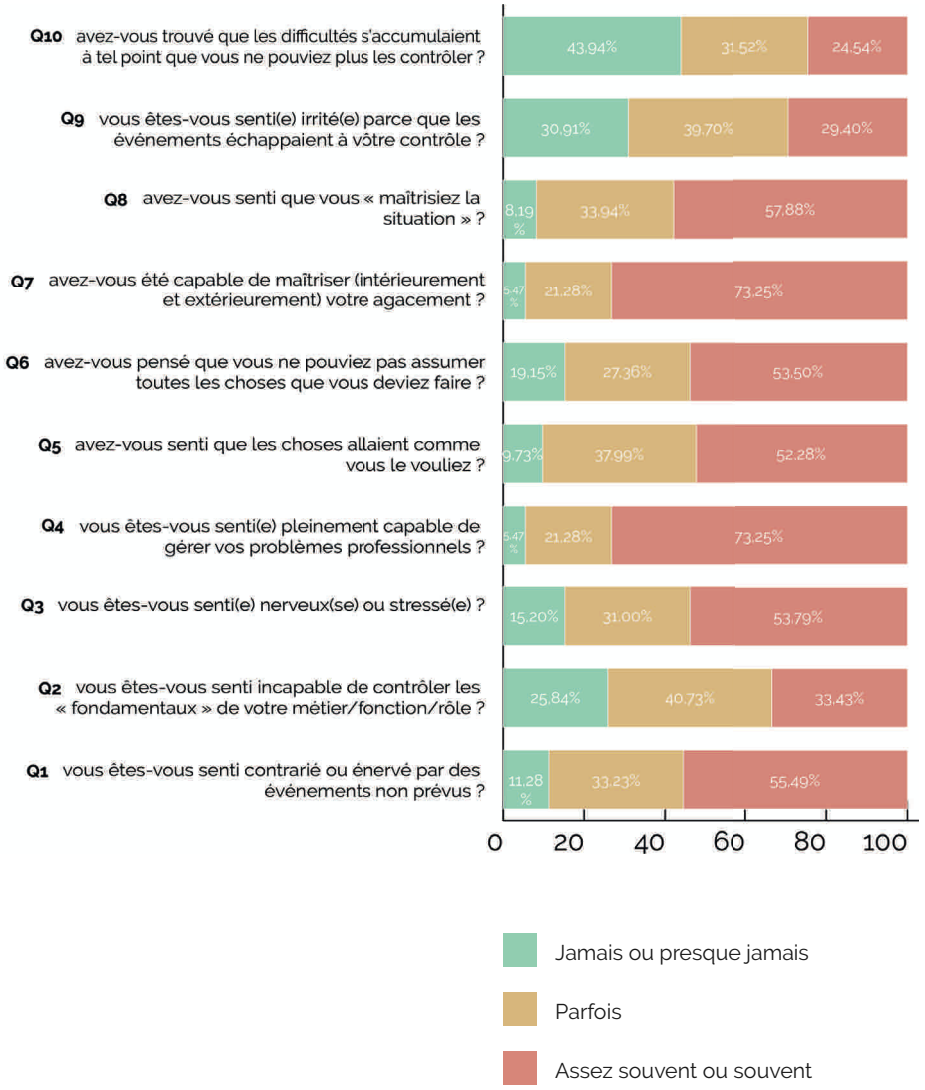
La première s'appuie sur les 10 questions du « PSS10 » (Perceived Stress Scale)

	Questions PSS10
1	Au cours du dernier mois vous êtes-vous senti contrarié ou énervé par des événements non prévus ?
2	Au cours du dernier mois vous êtes-vous senti incapable de contrôler les « fondamentaux » de votre métier/fonction/rôle ?
3	Au cours du dernier mois vous êtes-vous senti(e) nerveux(se) ou stressé(e) ?
4	Au cours du dernier mois vous êtes-vous senti(e) pleinement capable de gérer vos problèmes professionnels ?
5	Au cours du dernier mois avez-vous senti que les choses allaient comme vous le vouliez ?
6	Au cours du dernier mois avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?
7	Au cours du dernier mois avez-vous été capable de maîtriser (intérieurement et extérieurement) votre agacement ?
8	Au cours du dernier mois avez-vous senti que vous « maîtrisiez la situation » ?
9	Au cours du dernier mois vous êtes-vous senti(e) irrité(e) parce que les événements échappaient à vôtre contrôle ?
10	Au cours du dernier mois avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?

La deuxième s'appuie sur des questions mis en place par Advens et le CESIN spécifiquement pour l'étude.

	Questions sur les facteurs de stress liés au métier de la Cyber
13	Au cours du dernier mois avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?
14	Souffrez-vous de l'image et des a priori parfois négatifs autour de votre fonction, qui peuvent vous compliquer votre tâche voire provoquer un sentiment d'isolement ?
15	Avez-vous le sentiment d'être incompris(e) ou d'être jugé « excessif » lorsque vous faites des recommandations ?
16	Redoutez-vous les situations où votre métier vous amène à connaître des secrets et/ou vous place dans des contextes humainement délicats ou embarrassants ?
17	Ressentez-vous un manque d'expertise technique ou méthodologique ?
18	Estimez-vous difficile de devoir adapter en permanence vos analyses et stratégies devant un contexte de menace complexe et très évolutif, de devoir apprendre et vous réinventer sans cesse ?
19	Etes-vous à l'aise avec l'étendue fonctionnelle et technique que doit couvrir le métier cyber, qui doit assurer partout une défense efficace à tous les niveaux et sur tous les terrains ?
20	Trouvez-vous votre métier singulier, dans la mesure où il fait face à des adversaires, souvent « invisibles » et malveillants, ce qui est peu usuel, car peu de professions connaissent ce contexte d'adversité ?
21	Etes-vous frustré d'être uniquement du côté de la défense et de ne jamais pouvoir riposter ou contre-attaquer ?
22	Vous sentez-vous découragé devant l'augmentation de la fréquence et de la puissance des cyberattaques ?
23	Avez-vous un sentiment d'impuissance devant le caractère asymétrique du combat, l'attaquant ayant un net avantage sur le défenseur ?
24	Vous arrive-t-il de vous sentir personnellement en danger, devant cette adversité ?
25	Appréciez-vous les imprévus et les aléas, nombreux dans le métier ?
26	Êtes-vous perturbé(e) de ne pas connaître a priori, voire ne jamais connaître ceux qui vous attaquent ou commettent une action malveillante ?
27	Êtes-vous sur le qui-vive en permanence, sans pouvoir déconnecter vos pensées de votre travail, dans la crainte de la survenue d'une cyberattaque ou d'une situation à risque ?
28	Considérez-vous que votre situation professionnelle est incertaine, et qu'une crise majeure pourrait vous coûter votre poste ?
29	Est-ce que la gestion du risque Cyber vous parait un exercice intellectuellement difficile ?
30	Est-ce que vous vivez bien l'adrénaline, la pression et le sentiment d'urgence généralement associés à une crise Cyber ?
31	Appréciez-vous l'exercice périlleux, la balance permanente entre les décisions à prendre et les informations disponibles pour pouvoir les prendre, tout au long d'une crise ?
32	Vous sentez-vous compris ou a minima soutenu par vos proches pendant les périodes où vous gérez des crises ?
33	Comment ressentez-vous l'exercice de la communication, arrivez-vous à vous exprimer vraiment, à vous sentir en empathie, à convaincre vos interlocuteurs ?
34	Avez-vous le sentiment de devoir vous justifier auprès des autres, voire auprès de vous-même de l'utilité de vos actions ?
35	Est-ce que vous éprouvez un sentiment de culpabilité, lié (ou pas) au regard de votre entourage et/ou votre hiérarchie, lorsqu'un incident survient, et que vous n'avez pu l'empêcher, le détecter et/ou en limiter l'impact ?

10.2- Annexe 2 – Synthèse des résultats – PSS10



10.3- Annexe 3 – Synthèse des résultats – Facteurs de stress

		Non, pas du tout	Plutôt non	Plutôt oui	Oui, tout à fait
Coercition et surveillance	Q13 : Souffrez-vous de l'image et des a priori parfois négatifs autour de votre fonction, qui peuvent vous compliquer votre tâche voire provoquer un sentiment d'isolement ?	22,19%	39,82%	31,61%	6,38%
Coercition et surveillance	Q14 : Avez-vous le sentiment d'être incompris(e) ou d'être jugé « excessif » lorsque vous faites des recommandations ?	12,73%	40,00%	38,79%	8,48%
Coercition et surveillance	Q15 : Redoutez-vous les situations où votre métier vous amène à connaître des secrets et/ou vous place dans des contextes humainement délicats ou embarrassants ?	43,94%	39,70%	12,73%	3,64%
Complexité et évolutivité	Q16 : Ressentez-vous un manque d'expertise technique ou méthodologique ?	18,54%	41,64%	32,22%	7,60%
Complexité et évolutivité	Q17 : Estimez-vous difficile de devoir adapter en permanence vos analyses et stratégies devant un contexte de menace complexe et très évolutif, de devoir apprendre et vous réinventer sans cesse ?	12,77%	36,78%	37,08%	13,37%
Transversalité	Q18 : Etes-vous à l'aise avec l'étendue fonctionnelle et technique que doit couvrir le métier cyber, qui doit assurer partout une défense efficace à tous les niveaux et sur tous les terrains ?	2,43%	20,06%	54,10%	23,40%
Combat et adversité	Q19 : Trouvez-vous votre métier singulier, dans la mesure où il fait face à des adversaires, souvent « invisibles » et malveillants, ce qui est peu usuel, car peu de professions connaissent ce contexte d'adversité ?	5,17%	13,07%	46,20%	35,56%

Combat et adversité	Q20 : Etes-vous frustré d'être uniquement du côté de la défense et de ne jamais pouvoir riposter ou contre-attaquer ?	40,61%	31,52%	20,61%	7,27%
Combat et adversité	Q21 : Vous sentez-vous découragé devant l'augmentation de la fréquence et de la puissance des cyberattaques ?	20,97%	51,37%	23,40%	4,26%
Combat et adversité	Q22 : Avez-vous un sentiment d'impuissance devant le caractère asymétrique du combat, l'attaquant ayant un net avantage sur le défenseur ?	13,64%	36,67%	39,39%	10,30%
Combat et adversité	Q23 : Vous arrive-t-il de vous sentir personnellement en danger, devant cette adversité ?	40,30%	41,21%	15,76%	2,73%
Incertitude et inconnu	Q24 : Appréciez-vous les imprévus et les aléas, nombreux dans le métier ?	2,43%	19,45%	64,13%	13,98%
Incertitude et inconnu	Q25: Etes-vous perturbé(e) de ne pas connaître a priori, voire ne jamais connaître ceux qui vous attaquent ou commettent une action malveillante ?	35,56%	46,20%	15,50%	2,74%
Incertitude et inconnu	Q26 : Etes-vous sur le qui-vive en permanence, sans pouvoir déconnecter vos pensées de votre travail, dans la crainte de la survenue d'une cyberattaque ou d'une situation à risque ?	12,42%	34,85%	37,27%	15,45%
Incertitude et inconnu	Q27 : Considérez-vous que votre situation professionnelle est incertaine, et qu'une crise majeure pourrait vous coûter votre poste ?	16,67%	29,39%	33,64%	20,30%
Incertitude et inconnu	Q28 : Est-ce que la gestion du risque Cyber vous parait un exercice intellectuellement difficile ?	10,33%	27,96%	49,85%	11,85%
Gestion de crise	Q29 : Est-ce que vous vivez bien l'adrénaline, la pression et le sentiment d'urgence généralement associés à une crise Cyber ?	1,83%	14,63%	64,02%	19,51%

Gestion de crise	Q30 : Appréciez-vous l'exercice périlleux, la balance permanente entre les décisions à prendre et les informations disponibles pour pouvoir les prendre, tout au long d'une crise ?	2,12%	20,91%	63,94%	13,03%
Gestion de crise	Q31 : Vous sentez-vous compris ou a minima soutenu par vos proches pendant les périodes où vous gérez des crises ?	3,34%	15,20%	52,89%	28,57%
Communication et conviction	Q32 : Comment ressentez-vous l'exercice de la communication, arrivez-vous à vous exprimer vraiment, à vous sentir en empathie, à convaincre vos interlocuteurs ?	1,82%	14,85%	66,97%	16,36%
Responsabilité et culpabilité	Q33 : Avez-vous le sentiment de devoir vous justifier auprès des autres, voire auprès de vous-mêmes de l'utilité de vos actions ?	10,61%	30,00%	41,52%	17,88%
Responsabilité et culpabilité	Q34 : Est-ce que vous éprouvez un sentiment de culpabilité, lié (ou pas) au regard de votre entourage et/ou votre hiérarchie, lorsqu'un incident survient, et que vous n'avez pu l'empêcher, le détecter et/ou en limiter l'impact ?	15,20%	36,78%	39,51%	8,51%

Cyber stress

Une grande étude sur le stress des Responsables Cyber

Septembre 2021

Advens CYBERSECURITY

CESIN