Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Cybersécurité des machines et prévention des risques professionnels : état des lieux

Cybersecurity of machines and prevention of occupational risks : state of play

LAMY Pascal
INRS
Vandoeuvre, France
pascal.lamy@inrs.fr

PERRIN Nellie
INRS
Vandoeuvre, France
nellie.perrin@inrs.fr

GHADBAN Nisrine
INRS
Vandoeuvre, France
nisrine.ghadban@inrs.fr

Résumé — Avec l'industrie du futur, les machines industrielles peuvent être de plus en plus connectées et échanger des données à l'aide de différents canaux de communication, ouvrant la porte à une plus grande vulnérabilité face à des cyberattaques. L'aspect risque professionnel n'est pas souvent évoqué comme risque suite à une cyberattaque. Cependant, la publication du règlement machine 2023/1230 introduit les actes malveillants dans les exigences essentielles de santé et sécurité, ce qui va nécessiter sa prise en compte lors de la conception des machines. Le travail présenté au travers de cette communication est de faire un état des lieux, à l'aide d'une enquête par questionnaires, auprès des entreprises. Cette enquête a pour but d'appréhender la connectivité des machines, de recueillir les pratiques des entreprises en matière de cybersécurité ainsi que le ressenti des travailleurs sur le risque de cyberattaque et ses impacts pour leur santé et leur sécurité au travail.

Les premiers résultats, présentés ici, permettent de voir les tendances, dans l'industrie, de la considération du risque de cyberattaque. Ils seront utilisés en support à la construction d'une méthode d'analyse de risque cyber pour les machines et permettront aussi de caractériser les vulnérabilités des machines. A terme, ils serviront ainsi à prendre en compte ce risque dans l'évaluation des risques professionnels.

Mots-clefs — Cybersécurité, machines connectées, prévention des risques professionnels, questionnaire, ressenti

Abstract — With the industry of the future, industrial machines can be increasingly connected and exchange data via different communication channels, opening the door to greater vulnerability to cyber attacks. The occupational risk aspect is not often mentioned as a risk following a cyber-attack. However, the publication of machine regulation 2023/1230 introduces malicious acts into the essential health and safety requirements, which will require them to be taken into account when designing machines. The purpose of this paper is to take stock of the current situation, by means of a questionnaire survey of companies. The aim of the survey is to gain an understanding of machine connectivity, company practices in terms of cybersecurity, and workers' perceptions of the risk of cyber-attack and its impact on their occupational health and safety.

The initial results, presented here, reveal trends in the industry's consideration of the risk of cyber-attack. They will be used to support the construction of a cyber-risk analysis method for machines, and to characterize machine vulnerabilities. Ultimately, they will also be used to factor this risk into occupational risk assessments.

Keywords — Cybersecurity, connected machines, occupational risk prevention, survey, experience

I. INTRODUCTION

Nous nous intéressons ici aux machines telles que définies par (European Union, 2006) : un ensemble équipé d'un système d'entraînement, composé de pièces ou d'organes liés entre eux dont au moins un est mobile et qui sont réunis de façon solidaire en vue d'une application définie.

Il y a une dizaine d'années, de par leur faible niveau ou même leur absence de connexion aux réseaux ouverts, les machines se trouvaient plus ou moins épargnés et en conséquence les industriels peu préoccupés par ce risque. La cybersécurité concernait alors plus spécifiquement le système d'information de l'entreprise.

Pour les machines, l'émergence de l'Industrie du futur les rend plus sensibles aux cyberattaques, du fait de l'augmentation des accès possibles, ce que l'on appelle la surface d'attaque en cybersécurité. Un accès au plus bas niveau des composants des machines (capteurs, actionneurs) est ainsi rendu possible du fait de leur connexion au réseau du système d'information de l'entreprise. L'utilisation de composants ou capteurs connectés (IIoT pour Industrial Internet of Things) à des fins d'amélioration de la production renforce aussi les possibilités d'accès. Tout ceci ouvre alors plus facilement la porte à des attaques par vecteur numérique.

Généralement, les cyberattaques sont associées surtout à la perte de données du système d'information et ses conséquences pour l'entreprise. Désormais, on peut anticiper une évolution de la menace et des conséquences en termes de risques industriels mais aussi en termes de risques professionnels. En effet, pour les salariés, différents impacts peuvent être envisagés en cas de cyberattaque :

- D'abord, il peut y avoir un risque en cas de dommages matériels sur l'installation ou le processus industriel (par exemple explosion, émission de substances dangereuses).
- Ensuite, si une attaque altère une fonction de sécurité sur une machine, le salarié se retrouve alors non protégé par rapport au risque couvert par cette fonction de sécurité (par exemple le mouvement dangereux d'un élément mobile de la machine dont le salarié ne serait plus protégé par la fonction de sécurité).
- Il peut en outre y avoir un risque que des données fausses sur l'état de la machine soient affichées, qui vont tromper le salarié et le placer ou lui faire faire une action le menant dans une situation dangereuse.
- Si une attaque vient à rendre la machine défaillante, une intervention de la maintenance doit être réalisée pour la remise en marche, il peut y avoir un risque accru d'accident : une intervention non planifiée, sous la pression temporelle, est plus accidentogène qu'une intervention prévue.
- Enfin, la perte ou le vol de données et leurs conséquences sur le contenu du travail, de même que l'atteinte de l'image de l'entreprise, peuvent générer des risques psycho-sociaux

Une récente étude (Maggi et al., 2017) met en avant un impact possible d'une cyberattaque pour une installation robotisée, comme la modification de la vitesse de déplacement du robot dans un mode manuel, ce qui pourrait engager la sécurité du travailleur (risque de heurt avec le robot). Une autre étude (Anderson et al., 2018) a aussi montré des vulnérabilités sur des télécommandes industrielles sans fil, vulnérabilités qui pourraient être exploitées pour mener une attaque et donc mener à des risques pour le salarié. Différents scénarios sont présentés dans cette étude, allant de la possibilité de « rejouer » des commandes simples jusqu'à la totale prise de contrôle à l'aide de cette télécommande. En prenant ainsi contrôle d'une télécommande utilisée pour piloter les mouvements d'éléments mobiles d'une machine, des mouvements intempestifs peuvent être générés et venir créer un risque de heurt ou coincement pour le salarié.

Le risque cyber existe pour les systèmes industriels. Il a jusqu'alors concerné des secteurs comme l'énergie, l'industrie pétrolière ou gazière, l'eau, le transport et dans une moindre mesure l'industrie manufacturière. Cependant, au vu des changements liés à l'Industrie du futur et plus particulièrement la digitalisation des données, il devient un risque émergent (Héry & Malenfer, 2018) (Lamy, 2019) pour les systèmes manufacturiers ; les machines sont ainsi une proie plus facile face aux cyberattaques. En outre, dans le cadre d'une enquête sur la cybersécurité des usines intelligentes (Le monde Informatique 2022), de nombreux dirigeants affirment qu'ils ne seront pas en mesure de répondre efficacement aux cyberattaques dans leurs usines intelligentes et leurs sites de production.

Après cette introduction sur le contexte de la cybersécurité pour les machines, la section II replace le travail mené dans le cadre d'une étude engagée par l'INRS sur ce sujet de la cybersécurité et plus particulièrement sur la volonté de voir comment inclure l'analyse de risque cyber pour les machines dans l'évaluation des risques professionnels. Afin de construire une analyse de risque cyber dédiée aux machines, la section III présente pourquoi nous avons lancé une enquête par questionnaire, comment cette enquête a été réalisée et quelles analyses seront menées avec les données récoltées. La section IV présente les premiers résultats de cette enquête. Ce papier se termine avec une partie discussion, perspectives et conclusion.

II. CADRE PLUS GLOBAL DE CE TRAVAIL

Après avoir présenté les impacts possibles en terme de risques professionnels en cas de cyberattaque, nous précisons, dans cette section, l'objectif de l'étude qui a été engagée par l'INRS pour la prise en compte du risque cyber.

Ce travail s'insère dans une étude plus large commencée en 2023 au sein de l'INRS pour la prise en compte du risque de cyberattaque par un utilisateur de machines lors de l'évaluation des risques professionnels (Evaluation des risques-Document unique). Comme explicité ci-dessus, le salarié travaillant sur une machine peut être soumis à des risques suite à un acte malveillant sur cette machine. Afin de déterminer les risques professionnels induits par les risques cyber sur une machine, il faut tout d'abord mettre au point une démarche d'analyse de risque (AdR) cyber pour les machines. L'idée est de construire une démarche simple, pour les utilisateurs de machine, pour déterminer et estimer le risque de cyberattaque sur cette machine. Ce travail sera ensuite poursuivi pour voir comment contribuer à un rapprochement entre l'AdR cyber pour les machines (ARCM) et l'évaluation des risques professionnels et ainsi comment prendre en compte le risque cyber lors de l'évaluation des risques professionnels. En effet, rien n'existe actuellement pour mener une évaluation des risques professionnels incluant les risques cyber.

De façon générale, les AdR cyber exploitent les menaces (circonstances ou événements ayant le potentiel d'affecter les installations) et les vulnérabilités (faiblesses de sécurité d'un point de vue cyber). Ces menaces et vulnérabilités permettent de construire des scénarios de cyberattaque pertinents, pour en estimer ensuite les risques associés.

Cette analyse est primordiale pour définir les mesures de prévention cyber adaptées à mettre en place par l'entreprise et in fine, les moyens de prévention des risques professionnels associés. Cette démarche doit être accessible à un utilisateur (industriel ou préventeur), de façon à lui permettre de mener lui-même son analyse de risque cyber.

Afin de construire une analyse de risque cyber pour les machines et pour faire un état des lieux des pratiques en cybersécurité, nous avons mené une enquête par questionnaire que nous présentons ci-dessous dans la section III.

III. QUESTIONNAIRES POUR UN ETAT DES LIEUX DE LA CONNECTIVITE DES MACHINES ET APPRÉHENDER LES PRATIQUES EN CYBERSECURITE

A. Pourquoi une enquête par questionnaires ?

L'analyse de risque cyber nécessite la détermination de scénarios d'attaque. Ces scénarios exploitent les vulnérabilités et les moyens d'accès aux équipements et matériels (Flaus, 2019). Ceci nécessite de comprendre la surface d'attaque c'est-à-dire comment les machines sont accessibles pour une cyberattaque, comment elles sont utilisées (par exemple utilisation de clé USB, programmation à distance, télémaintenance), et comment elles sont ou peuvent être connectées. Ces usages sont recueillis au travers d'une enquête basée sur 3 questionnaires : un premier destiné aux personnels de production et HSE, un second destiné aux personnels de maintenance et des bureaux des méthodes-travaux neufs, et un troisième destiné aux personnels du service informatique. L'objectif est d'une part de mieux comprendre les vulnérabilités et les points d'entrée pour les machines et d'autre part d'exploiter ces informations afin de proposer des actions élémentaires « génériques » pour la construction de scénarios d'attaque sur les machines, actions qui contribueront ainsi à réaliser cette AdR cyber pour les machines (ARCM). De fait, cette ARCM n'est pas présentable ici.

B. Réalisation, validation et diffusion des questionnaires

Les trois questionnaires ont été élaborés en pluridisciplinarité avec une ergonome-psychologue du travail. En s'appuyant sur l'expertise de collègues ingénieurs INRS, les questionnaires ont été construits autour d'hypothèses préalablement réfléchies telles que :

- Hypothèse 1 - Les machines sont généralement connectées
- Hypothèse 2 - Les salariés ont peu conscience du risque de cyberattaque
- Hypothèse 3- Les entreprises ne prennent pas forcément en compte le risque de cyberattaque
- Hypothèse 4- En cas de cyberattaque, les personnes craignent principalement les conséquences matérielles et une perturbation de la production plutôt que des effets sur leur santé et leur sécurité
- Hypothèse 5- Peu d'entreprises ont subi une cyberattaque
- Hypothèse 6 – En cas de cyberattaque subie par l'entreprise, les conséquences sont multiples

Chaque questionnaire possède un tronc commun et des parties spécifiques au public cible :

- Informations générales (profil du répondant et de l'entreprise),
- La connectivité des machines (réseaux, serveurs, port USB, etc.)
- L'accessibilité aux machines (physique ou à distance)
- Les équipements, logiciels et sécurité de la machine (programmation, automate de sécurité etc.)
- La cybersécurité (sensibilisation, formations, moyens de protection, etc.)
- Les conséquences d'une cyberattaque (retour d'expérience, moyens de gestion de la crise, affects, etc.)

Les questionnaires sont composés de plusieurs items visant à recueillir le point de vue des personnes sur la survenue potentielle d'une cyberattaque et leur ressenti lorsqu'ils en ont été victimes. Le nombre d'items varie de 39 à 61 selon le

questionnaire. Les modalités de réponses aux items sont présentées principalement sous la forme d'échelles de Lickert allant de 1 « Pas du tout d'accord » à 4 « Tout à fait d'accord » ou de listes de choix, permettant des réponses rapides et facilement exploitables statistiquement.

Les questionnaires ont fait l'objet d'une validation qualitative (validation de contenu et test de compréhension) (Bouletreau et al. 1999). Celle-ci est basée dans un premier temps sur le jugement d'experts constitués d'ergonomes/psychologues du travail internes à l'INRS sans lien avec cette étude. Ces experts ont apporté une appréciation subjective quant à l'absence de dérive par rapport à l'objectif initial, la structure du questionnaire (il ne doit pas être une juxtaposition de questions mais un tout, les questions devant suivre un ordre logique), la compréhension des questions par la population cible, la non-induction des réponses, la pertinence des modalités de réponse, le choix des réponses et leur nombre, la non-ambiguïté du vocabulaire et l'utilité de toutes les questions afin de réduire au maximum la longueur du questionnaire. Dans un second temps, les questionnaires ont été testés auprès de différentes personnes représentatives des publics cibles permettant de s'assurer de la formulation compréhensible des questions. La prise en compte des remarques a permis la validation définitive des questionnaires. Ils ont été ensuite transposés sous une forme électronique, à l'aide du logiciel Sphinx iQ3. Ce logiciel permet de concevoir des questionnaires en ligne et de réaliser les premières analyses descriptives. L'utilisation d'un questionnaire en ligne permet de faciliter sa diffusion et de s'assurer du caractère anonyme et confidentiel des réponses.

La diffusion des questionnaires a été réalisée au travers des moyens de communication et de diffusion accessibles pour l'INRS. Nous avons ainsi utilisé le réseau des préventeurs des CARSAT, qui par leur contact direct en entreprise, peuvent toucher les publics visés. Des publicités ont été faites dans certains périodiques de l'INRS, sur le site Web ainsi que sur les réseaux sociaux. Différentes associations ont été sollicitées pour diffuser telles que IMdR, Exera, CLUSIR, CESIN. L'idée est de diffuser de façon large pour permettre le plus de retours de la part des entreprises utilisant des machines.

C. Analyses envisagées

Un traitement statistique des réponses aux questionnaires permettra de répondre aux hypothèses précédemment construites.

Une analyse statistique descriptive (modes, moyennes, écart-types, etc.) est prévue via le logiciel Sphinx iQ3. Les données feront également l'objet d'un traitement statistique complémentaire avec le logiciel Stata V17. Des analyses de variance (Anova) pour comparer des variables entre elles et des analyses inférentielles (corrélation de Spearman, régression linéaire hiérarchique) pour mettre en évidence des corrélations entre variables ou expliquer certains résultats pourront être réalisées.

Après avoir présenté l'objet de cette enquête, comment nous l'avons réalisée et les analyses envisagées, nous donnons ci-dessous, en section IV, les premiers résultats issus du questionnaire production, profil donnant le plus grand nombre de réponses.

IV. PREMIERS RESULTATS

L'enquête est ouverte jusque septembre 2024 et le traitement statistique complet ne pourra être effectué qu'ensuite. Nous ne pouvons donc présenter ici qu'une partie de l'analyse descriptive des réponses obtenues à ce jour. Les résultats présentés sont ceux du questionnaire « production » et permettent de répondre aux exemples d'hypothèses présentées ci-dessus (§III B).

A. Contexte des réponses et connectivité des machines

A ce jour, 45 personnes ont répondu au questionnaire « production ». Ce questionnaire est destiné autant au personnel de production qu'au personnel QHSE. Globalement, les répondants au questionnaire sont des personnels QHSE (51%) (Fig.1). La catégorie « Autre » est composée d'automaticien, cariste, métrologue.

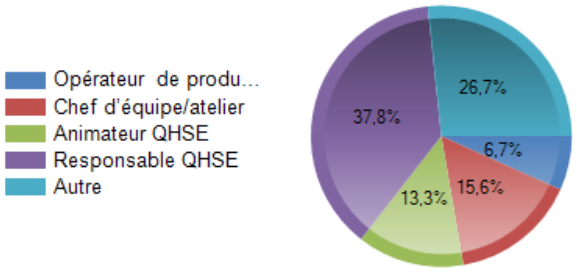


Fig. 1 : Répartition des répondants

1) Résultat de l'hypothèse 1 : Les machines sont généralement connectées

Pour ce qui concerne la connectivité des machines de façon générale, les résultats ci-dessous (Fig. 2) montrent que la majeure partie des machines sont connectées au réseau, ce qui les rend susceptibles d'être accessibles pour une cyberattaque.

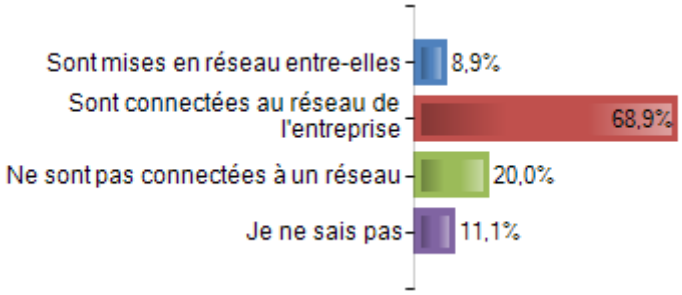


Fig. 2. Connection des machines au réseau

B. Résultat de l'hypothèse 2 - Les salariés ont peu conscience du risque de cyberattaque

Pour ce qui concerne la sensibilité des personnes à la cybersécurité, 96% des répondants déclarent se sentir concernés par cette problématique de cyberattaque (Table 1), ce qui tend à montrer une certaine conscience de ce risque.

Table 1. Sensibilité à la cybersécurité

Vous vous sentez concernés par la cybersécurité :

	Effectifs	% Obs.
Pas du tout d'accord	0	0%
Plutôt pas d'accord	2	4,4%
Plutôt d'accord	21	46,7%
Tout à fait d'accord	22	48,9%
Total	45	100%

C. Résultats de l'hypothèse 3- Les entreprises ne prennent pas forcément en compte ce risque de cyberattaque

L'entreprise communique ou parle de ce risque de cyberattaque et met en place des mesures, ce qui montre la préoccupation des entreprises face à ce risque.

En effet, 90% des répondants déclarent entendre parler de risque cyber (Table 2). Toutefois 20% des répondants déclarent ne pas avoir été sensibilisés ou peu au risque de cyberattaque (Table 3).

Table 2. - Dans votre entreprise, vous entendez parler de risques cybersécurité :

	Effectifs	% Obs.
Pas du tout d'accord	2	4,4%
Plutôt pas d'accord	2	4,4%
Plutôt d'accord	13	28,9%
Tout à fait d'accord	28	62,2%
Total	45	100%

Table 3- Vous avez été sensibilisé à la cybersécurité :

	Effectifs	% Obs.
Pas du tout d'accord	5	11,1%
Plutôt pas d'accord	4	8,9%
Plutôt d'accord	15	33,3%
Tout à fait d'accord	21	46,7%
Total	45	100%

Le risque de cyberattaque est pris en compte dans l'entreprise pour 87% des répondants (Table 4). Ceci ne semblait pas une évidence avant la réalisation de cette enquête, notamment pour les TPE-PME puisqu'une étude d'Advisor Smith (J'automatise 2023) a montré que 83% des dirigeants de PME n'ont toujours pas mis en œuvre une stratégie de cybersécurité.

Table 4 - Le risque de cyberattaque est pris en compte dans l'entreprise :

	Effectifs	% Obs.
Oui	39	86,7%
Non	2	4,4%
Je ne sais pas	4	8,9%
Total	45	100%

Cependant, la prise en compte du risque de cyberattaque dans l'évaluation des risques professionnels est encore timide. En effet, 46% des répondants déclarent que le risque de cyberattaque n'est pas pris en compte dans l'évaluation des risques et 23% ne savent pas s'il l'est (Table 5). Ce résultat est paradoxal puisque 91% des répondants pensent qu'une cyberattaque est possible dans l'entreprise (Fig. 3).

Table 5 - Il est pris en compte dans l'évaluation des risques professionnels :

	Effectifs	% Obs.
Oui	12	30,8%
Non	18	46,2%
Je ne sais pas	9	23,1%
Total	39	100%

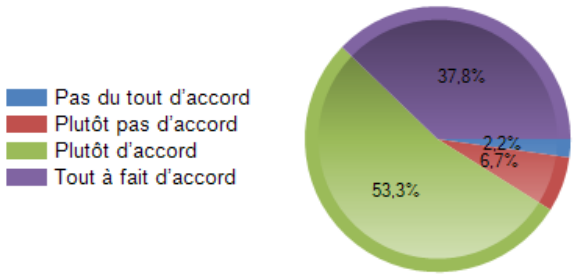
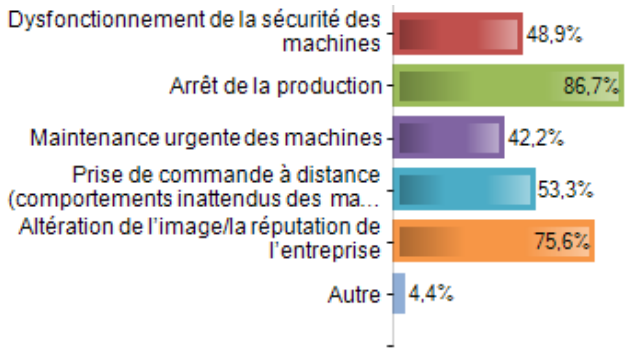


Fig. 3 – Vous pensez qu'une cyberattaque est possible dans votre entreprise

D. Résultats de l'hypothèse 4 : En cas de cyberattaque, les personnes craignent principalement les conséquences matérielles et une perturbation de la production plutôt que des effets sur leur santé et leur sécurité

Lorsque l'on interroge le personnel sur les conséquences d'une cyberattaque, ce sont les arrêts de production ou l'altération de l'image de l'entreprise qui sont mis en avant pour respectivement 87% et 76% des répondants (Fig. 4). En interrogeant spécifiquement sur les conséquences en terme de SST, 85% des répondants envisagent des conséquences SST (Fig. 5). Bien que 42% des personnes considèrent qu'une cyberattaque puisse causer des dommages corporels, ils sont 79% à craindre surtout pour leur emploi (Fig. 6).



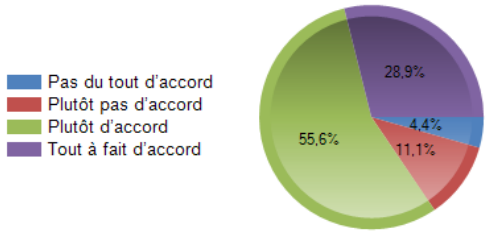


Fig. 4 –Conséquences sur l'entreprise

Fig. 5 - Une cyberattaque peut affecter la santé/sécurité

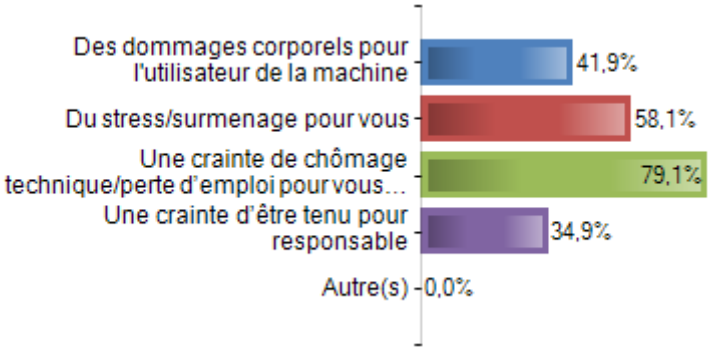


Fig.6 - La cyberattaque pourrait générer

E. Résultats de l'hypothèse 5 : Peu d'entreprises ont subi une cyberattaque

15 personnes sur 45 déclarent avoir vécu une cyberattaque (Table 6).

Table 6 - Une cyberattaque a déjà eu lieu au sein de votre entreprise :

	Effectifs	% Obs.
Oui	15	33,3%
Non	13	28,9%
Je ne sais pas	17	37,8%
Total	45	100%

F. Résultats de l'hypothèse 6 – En cas de cyberattaque subie par l'entreprise, les conséquences sont multiples

47% des répondants estiment qu'une cyberattaque peut altérer le fonctionnement général de l'entreprise. Les conséquences d'une cyberattaque sont diverses et peuvent impacter autant le système d'information (perturbation du réseau : 67%, perte d'accès aux serveurs : 67%, pertes de moyens de communication : 60%, vols de données : 33%) que la logistique (20%) et les machines (27%) (Fig. 7).

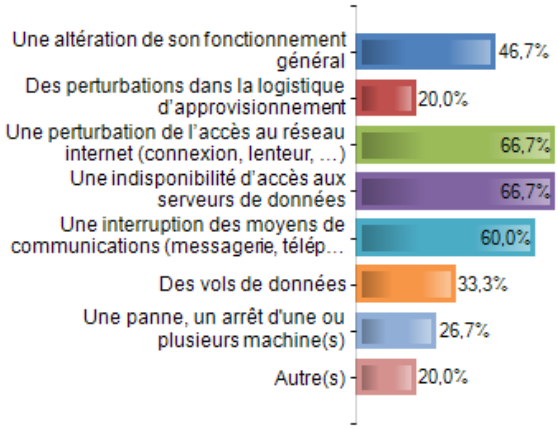


Fig. 7. L'entreprise a subi

20% des personnes ayant subi une cyberattaque indiquent s'être senties en insécurité (Fig. 8). 67% ont déclaré que leur travail a été perturbé plusieurs jours voire plusieurs mois (Fig. 9) et 27% se sont senties stressées suite à celle-ci (Fig. 10).

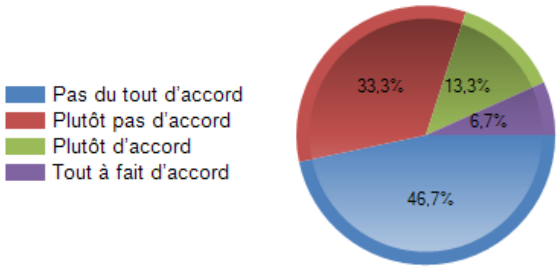


Fig. 8 – Vous vous êtes senti en insécurité pendant l'attaque

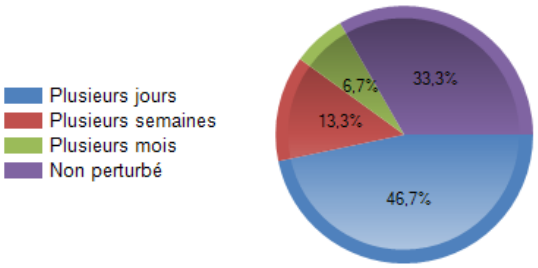


Fig. 9. Votre travail a été perturbé pendant

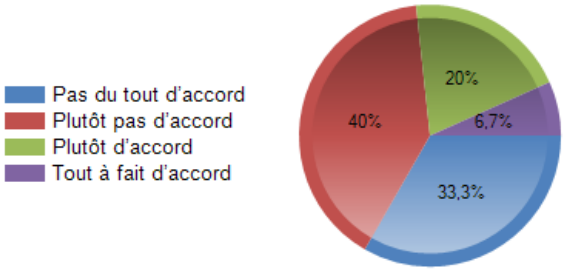


Fig. 10 – Vous vous êtes senti stressé suite à l'attaque

Après cette présentation des résultats, nous les discutons dans la section V suivante pour faire ressortir les points qui nous semblent pertinents.

V. Discussion et perspectives

L'enquête étant en cours, les résultats sont à prendre avec précaution. Nous souhaitons vérifier, au travers de cette enquête, certaines positions relatées par les médias (cf. IV C) telles que la lenteur des entreprises à prendre en compte le risque de cyberattaque (peu de moyens humains ou techniques).

Les machines industrielles sont généralement reliées au réseau et peuvent être sujettes à une cyberattaque, par différents vecteurs : réseau, port USB, accès à distance. Dans un monde industriel en pleine évolution avec un partage ou un échange de données à l'aide de différents moyens, le risque de cyberattaque augmente pour les machines industrielles et nécessite de s'interroger sur sa prise en compte.

Les premiers résultats montrent que les entreprises semblent sensibilisées au risque de cyberattaque et qu'elles le prennent en considération. La tendance de ces réponses s'explique peut-être par une forte présence de personnels QHSE dans les répondants à ce questionnaire. De même, 30% des répondants ont déjà vécu une cyberattaque et ont donc dû se protéger. Cependant, bien que les entreprises se déclarent sensibilisées sur le sujet, près de la moitié des répondants ont déclaré que le risque de cyberattaque ne figurait pas dans l'analyse des risques professionnels (SST). Des améliorations restent donc à apporter pour une meilleure prévention des risques professionnels.

Concernant les conséquences d'une cyberattaque, l'enquête met en évidence des conséquences matérielles mais pas uniquement. Les répondants craignent à la fois pour leur sécurité physique (dommage corporel suite à un risque mécanique) mais également pour leur bien-être psychologique avec des répercutions sur l'image de l'entreprise, une crainte de la perte de leur emploi, une perturbation de leur travail ou encore du stress.

Les analyses de cette enquête se poursuivent, comme précisé dans le III.C avec un traitement statistique plus complet. Les résultats donneront lieu à d'autres communications ou publications. Par ailleurs, ils seront exploités pour contribuer à la réalisation de l'analyse de risque cyber pour les machines (ARCM), en permettant de dégager et préciser, par exemple, des vulnérabilités génériques pour les machines.

VI. Conclusion

Les résultats de cette enquête confirment la présence du risque de cyberattaque en milieu industriel. Les entreprises semblent sensibilisées à ce risque et actives dans sa prise en charge. Les conséquences pouvant être graves pour la bonne marche de l'entreprise, il semble logique qu'elle le prenne en considération. Par contre, la prise en compte du risque cyber en terme de SST peut être améliorée : les évaluations des risques professionnels menées par les entreprises ne l'envisagent généralement pas. Ceci nous conforte dans la suite des travaux menés par l'INRS, visant à voir comment intégrer le risque cyber dans l'évaluation des risques professionnels pour les machines.

REMERCIEMENTS

Nous remercions toutes les personnes qui ont participé à cette enquête et celles qui auront permis la diffusion du questionnaire au sein des entreprises, notamment les ingénieurs et contrôleurs de sécurité des services prévention des accidents du travail et des maladies professionnelles des Caisse d'Assurance Retraite et de la Santé au Travail (CARSAT).

References

Anderson, J., Balduzzi, M., Hilt, S., Lin, P., Maggi, F., Urano, A., & R., V. (2018). *A security analysis of radio remote controllers for industrial applications*. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf

Bouletreau, A., Chouaniere, D., Wild, P., Fontana, J.M. (1999). *Concevoir, traduire et valider un questionnaire. A propos d'un exemple, EUROQUEST.*. [Rapport de recherche] Notes scientifiques et techniques de l'INRS NS 178, Institut National de Recherche et de Sécurité (INRS). 46 p., ffhal01420163f

European Union (2006). Directive 2006/42/EC of the European parliament and of the council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast).

Flaus, J.-M. (2019). *Cybersécurité des systèmes industriels*: ISTE Editions.

Héry, M., & Malenfer, M. (2018). Evolution des modes de production et risques professionnels : un état des lieux de la veille en 2017. *HST, 251*, 108-115.

J'Automatise n°145 (2023). *Dossier cybersécurité-Pourquoi les TPE-PME doivent prendre la cybersécurité au sérieux*

Lamy, P. (2019). Sécurité des machines : le risque cyber comme risque émergent? *HST, 256*, 72-79.

Le monde informatique (2022) Les usines connectées ne sont pas préparées aux cyberattaques - Le Monde Informatique

Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A. M., & Zanero, S. (2017). *Rogue Robots: Testing the Limits of an Industrial Robot's Security*. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security