La perception du risque cyber en entreprise : conception d'un cyberscore professionnel à destination des dirigeants

Emilie Peneloux, Philippe Lépinard, Cécile Godé

La perception du risque cyber en entreprise : conception d'un cyberscore professionnel à destination des dirigeants

Émilie Peneloux[1] *Philippe Lépinard*[2] *Cécile Godé*[1]
[1]Aix-Marseille Université, CRETLOG, F-13080 Aix-en-Provence, France
[2]Univ Paris Est Créteil, IRG, F-94010 Créteil, France

Résumé :

Entrée en vigueur le 1er octobre 2022, la loi n°2022-309 pour la mise en place d'une certification de cybersécurité des plateformes numériques est destinée au grand public afin que les usagers puissent prendre conscience des risques cyber lorsqu'ils recourent à des prestations numériques. Notre projet de recherche[1]souhaite prolonger cette démarche dans un contexte professionnel afin de déterminer si un tel dispositif peut également influencer la perception des risques cyber au niveau de la Direction d'une organisation. Notre objectif est donc la construction d'un instrument de gestion (cyberscore) selon une approche de type *Design Science Research* (DSR). Cet article présente les travaux préliminaires de notre recherche et les axes d'approfondissements que nous souhaitons développer et discuter dans le cadre de la conférence annuelle de l'AIM.

Mots clés :

Cyberscore ; Risque Cyber ; Perception du risque ; Cybersécurité

The perception of cyber risk in companies: design of a professional cyberscore for executives

Abstract :

The law n°2022-309 for the implementation of a cybersecurity certification of digital platforms, which came into force on October 1st, 2022, is intended for the general public so that users can become aware of cyber risks when they use digital services. Our research project, wishes to extend this approach in a professional context in order to know if such a system can also

[1] Issu d'un premier travail de mémoire de Master 2 (Peneloux, 2022) et poursuivi dans le cadre d'une thèse CIFRE.

influence the perception of cyber risks at the level of the top management of an organization. Our objective is therefore to build a management tool (cyberscore) using a Design Science Research (DSR) approach. This article presents the preliminary work of our research and the areas of research that we would like to develop and discuss at the AIM annual conference.

Keywords :
Cyberscore ; Cyber risk ; Risk perception ; Cybersecurity

La perception du risque cyber en entreprise : conception d'un cyberscore à destination des dirigeants

1. Introduction

Selon Mishra (2022, p. 45), « *cybersecurity refers to the process and methodologies designed and implemented to protect organization data from any cyberattack (through the mode of the internet), ensuring the CIA* [Confidentialité, Intégrité, Disponibilité, NDA] *of the information is maintained* ». Dans ce contexte, le 3 mars 2022, le Président de la République française promulguait la loi n°2022-309 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public[2]. Entrée en vigueur le 1er octobre 2022, la loi précise que le résultat d'un audit de cybersécurité réalisé par un prestataire agréé de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) doit être « *présenté au consommateur de façon lisible, claire et compréhensible et est accompagné d'une présentation ou d'une expression complémentaire, au moyen d'un système d'information coloriel* »[3]. Sans qu'il en soit fait explicitement mention, une analogie avec le Nutri-score est réalisée, le terme largement utilisé pour parler de la présentation des résultats de cet audit est le "Cyberscore"[4] (Figure 1). À ce jour, les critères de notation et la signification des différents niveaux du cyberscore ne sont pas encore définis. Sa finalité est cependant claire : le cyberscore doit être un outil d'aide à la décision grand public, qui doit permettre aux usagers de percevoir le niveau de risques cyber auquel ils sont exposés lorsqu'ils recourent à des prestations numériques[5].

Définit comme "*la combinaison de la probabilité d'un événement dans le domaine des Systèmes d'Information en réseau et des effets de cet événement sur les actifs et la réputation d'une organisation* » (World Economic Forum, 2012, p. 24), un risque cyber est par nature

---

[2] Lien vers le texte de loi : https://bit.ly/3irboXZ (consulté le 04 décembre 2022).

[3] Le récent texte européen « Un niveau élevé commun de cybersécurité dans l'ensemble de l'Union » (P9_TA(2022)0383), sans aborder la notion de cyberscore, fait d'ailleurs référence à ce besoin de sensibilisation « *La sensibilisation à la cybersécurité et la cyberhygiène sont essentielles pour améliorer le niveau de cybersécurité au sein de l'Union, compte tenu notamment du nombre croissant de dispositifs connectés qui sont de plus en plus utilisés dans les cyberattaques. Des efforts devraient être consentis pour améliorer la prise de conscience globale des risques liés à ces dispositifs, tandis que les évaluations au niveau de l'Union pourraient contribuer à garantir une compréhension commune de ces risques au sein du marché intérieur* » (p.37), https://bit.ly/3GsR2p5 (consulté le 4 décembre 2022).

[4] « *Nutri-Score est un repère graphique. Il classe chaque produit selon un score qui prend en compte la teneur en nutriments et aliments à favoriser et ceux à limiter. Son calcul consiste à faire la différence, pour 100 grammes de produit, entre les composantes négatives (sucres, sel, acides gras saturés...) et positives (vitamines, fibres, protéines,...) d'un aliment et permet d'attribuer une note. Celle-ci est alors transcrite sur une échelle de 5 couleurs (du vert foncé au orange foncé), associées à des lettres allant de A (« meilleure qualité nutritionnelle ») à E (« moins bonne qualité nutritionnelle)* » (Définition issue du Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, https://bit.ly/3GnUmC5, consulté le 4 décembre 2022).

[5] Netter (2022, p.309) n'hésite pas toutefois à indiquer que « *le cyberscore qui aura été publié pourra contribuer à éclairer leur* (les entreprises, NDA) *choix de prestataire : quand bien même il a été conçu pour les consommateurs, il pourra être connu de tous. Or, on ne voit pas pourquoi les résultats d'un audit de cybersécurité n'intéresseraient que les clients particuliers* ».

stratégique : il peut s'avérer létal « *pour une organisation, avec une fulgurance effrayante* » (Salamon, 2020, p. 103). C'est également un risque systémique qui *"porte à la fois sur une organisation mais aussi plus largement sur l'ensemble de l'écosystème utile à son fonctionnement* » (*ibid*., p.104). Cette communication interroge les effets d'un cyberscore développé au sein d'une banque coopérative sur la perception des risques cyber par les dirigeants.

Figure 1. Possible représentation du Cyberscore (©IT for Business).

2. Terrain de recherche

Notre recherche se déroule au sein de la CASDEN Banque Populaire[6] rattachée au Groupe Banques Populaires et Caisses d'Épargne (BPCE). Cette banque coopérative est une entreprise du secteur de l'économie sociale et solidaire. L'organisation ne possède pas de moyen de paiement mais accompagne ses sociétaires dans leurs projets en leur proposant une offre globale d'épargne, de crédits et de caution. Cela se fait dans le cadre d'un partenariat avec les Banques Populaires du Groupe, ce qui permet aux Sociétaires de bénéficier d'une offre bancaire complète et de proximité. Le Groupe BPCE est le deuxième Groupe bancaire en France en 2020 et la CASDEN en détient 2,86% du capital. La plupart des entités de BPCE ont des systèmes d'information (SI) infogérés par le Groupe. Ce n'est pas le cas de la CASDEN qui a son propre SI. La CASDEN doit donc être capable d'offrir un haut niveau de sécurité à la fois pour protéger les données de ses clients mais et préserver l'image et la réputation du Groupe. De plus, comptant un peu moins de 900 collaborateurs en 2022, c'est une organisation "à taille humaine", où la direction et les responsables restent accessibles. Ces paramètres en font un terrain de recherche et d'expérimentations particulièrement intéressant, alliant les problématiques liées à la gouvernance de la sécurité des systèmes d'information (SSI) des grands Groupes et la proximité organisationnelle des ETI.

3. La perception du risque cyber

Hohenemser et *al.* (1985) définissent le risque comme la combinaison de deux facteurs : la probabilité d'un préjudice et l'étendue de la menace. Ces éléments se retrouvent lorsqu'il s'agit de caractériser un risque lié aux SI, plusieurs auteurs insistant sur la probabilité d'occurrence d'un événement indésirable et l'ampleur de ses conséquences (Bandyopadhyay, et *al.*, 1999 ; Dhillon, et *al.*, 2006 ; Albrechtsen, et *al.*, 2009). La perception du risque est une notion inhérente au concept de risque. L'ampleur d'une menace pour un individu est biaisée par sa propre perception de la réalité. Ainsi, la perception du risque est-elle considérée comme

[6] Site internet de la CASDEN Banque Populaire : https://www.casden.fr/.

subjective et le risque comme socialement construit (Slovic, 1999). À la suite des travaux de Slovic, Sjöberg et *al.* (2004) définissent la perception du risque comme l'évaluation subjective de (1) la probabilité qu'un événement survienne et (2) ses impacts. La perception du risque conduit à prendre une décision en lien avec l'acceptabilité du risque. C'est même sa seule finalité selon Yates & Stone (1992). Agir sur la perception du risque cyber permettrait donc d'agir sur la décision quant à l'acceptabilité ou non du risque et donc de sa gestion.

La littérature en management des SI contribue depuis de nombreuses années aux problématiques de sécurité des SI (SSI) et de perception des risques SI. Nous identifions à ce jour onze travaux majeurs mobilisant principalement le cadre théorique de la perception cognitive du risque (Goodhue, et *al.*, 1991 ; Loch, et *al.*,1992 ; Straub, et *al.*, 1998 ; Taylor, 2006 ; Tsohou et *al.*, 2006 ; Albrechtsen, 2007 ; McFadzean et *al*., 2007 ; Barlette, 2008 ; Albrechtsen et *al.*, 2009 ; Barlette et *al.*, 2019 et Ogbanufe et *al.*, 2021). Ces contributions ont en commun d'insister sur l'écart existant entre les besoins de SSI et les mesures mises en place dans les organisations (Loch et *al.*, 1992). Reix et *al.* (2011) vont plus loin en pointant la nécessité d'une approche globale du risque SSI et de l'engagement de la Direction Générale : « *pour les responsables, la gestion de la sécurité se situe dans un univers incertain ; certains sinistres résultent de combinaisons difficilement envisageables de causes variées […] Ces deux difficultés justifient une approche globale du problème de la sécurité des SI* » (p. 435).

Cependant, force est de constater que la Direction n'est pas impliquée, ou pas suffisamment, dans la gestion du risque SSI (Grover, 1993 ; Avolio, 2000 ; McFadzean et *al.*, 2007). La conséquence est une délégation de ce risque à des experts (McFazdean et *al.*, 2007) internes ou externes à l'organisation, créant un « faux sentiment de sécurité » lié à cette délégation. Cela conduit à des solutions de réduction du risque mises en place de manière souvent trop hâtive et non-alignée avec la stratégie générale de l'organisation (McFadzean et *al*., 2007, p. 654). Cette situation n'est pas nouvelle puisqu'en en 1998, Straub & Welke soulignaient déjà la connaissance partielle de la Direction concernant les mesures de sécurité existantes et comment cela conduisait à limiter son intérêt pour les risques SI. Ce clivage entre experts et profanes (Slovic, 1987) dans la perception du risque SI rend difficile la gestion d'un risque global délégué à des experts. Les travaux mentionnés précédemment ne se penchent pas encore sur la spécificité du risque cyber. C'est ce que s'attache à faire cette recherche.

4. Méthodologie

Notre objectif est la construction d'un instrument de gestion que nous nommerons pour l'instant « cyberscore pour applicatifs métiers » (CAM). La construction d'un tel artefact nécessite une bonne connaissance du parc informatique de l'entreprise et donc un premier niveau de maturité cyber. L'objectif étant qu'il soit réalisé en interne par les gestionnaires de risques et non par un tiers externe comme pourrait l'être un audit. Pour ce faire, nous avons choisi une approche de type *Design Science Research* (DSR). Cette science de la conception a été notamment étudiée par Simon en 2004 et peut être définie comme « *un paradigme de recherche dans lequel un concepteur répond à des questions relatives à des problèmes humains par la création d'un artefact innovant tout en contribuant par l'apport de connaissances nouvelles à l'ensemble des preuves scientifiques* » (Hevner & Chatterjee, 2010, p. 5). Simon stipule également que « *la forme de la conception elle-même, et l'organisation du processus de la conception, sont l'une*

et l'autre deux composantes essentielles d'une théorie de la conception » (2004, p. 234). Le DSR est axé sur la résolution de problèmes via la création et le positionnement d'un artefact dans son environnement (Baskerville, 2008), ce qui nous semble correspondre à notre intention de recherche.

5. Résultats préliminaires

Un prototype de CAM a été construit au sein de la CASDEN Banque Populaire et proposé à neuf dirigeants de premier niveau et a concerné une application catégorisée comme vitale puisque permettant la prise de contact avec la clientèle. La valeur métier de cette application est donc très forte et un incident de sécurité sur cette dernière et ses données entraînerait des impacts forts pour l'organisation (perte de clientèle, perte financière, impact sur l'image, dysfonctionnements organisationnels, etc.). Cette application, après calcul sur les cinq critères[7] (Tableau 1)[8], a obtenu la note de D (sur E). Cette note a été présentée en comité. Le CAM et le projet dans son ensemble ont été ensuite approfondis lors d'entretiens semi-directifs.

Critère	Définition
État des vulnérabilités sur les serveurs	Score calculé à partir d'un logiciel donnant la totalité des vulnérabilités et leur criticité sur chaque brique technique d'une application
Revues d'habilitations réalisées sur l'année	Nombre de revues réalisées pour une application donnée chaque année
Taux de *patch management* Linux et Windows	Nombre de patchs de sécurité correctement passés sur les serveurs Linux et Windows d'une application
Taux d'antivirus à jour Linux et Windows	Taux d'antivirus à jour sur les serveurs Linux et Windows
Obsolescence des systèmes d'exploitation (SE/OS)	Taux d'OS pris en charge par l'éditeur (l'éditeur propose des patchs de sécurité pour ces versions)

Tableau 1. Les 5 critères retenus pour le prototype.

Les résultats préliminaires obtenus sont encourageants car nous constatons un écart entre leur perception du risque cyber avant et après la présentation du prototype. À l'issue de la construction et de la présentation du cyber-score, les responsables SI expriment l'intention de mettre en place des plans d'actions et autres dispositifs de remédiation du risque. Des ressources, comme des jours-personnes, du budget ou de la planification, discutés tant du côté SSI et que de celui des métiers. Des changements de comportements et une appropriation du domaine cyber sont également observés chez les deux parties, SSI et Direction. Les responsables métiers évoquent la mise en place de pratiques allant dans le sens des attentes SSI

[8] Le choix des critères s'est fait sur des aspects rapidement opérationnalisables durant l'année de Master 2. Dans le cadre de notre recherche, il s'agira d'identifier des critères plus pertinents et, peut-être, en lien avec l'apparition des critères du CyberScore grand public.

comme la mise à jour régulière de patchs de sécurité ou l'intégration de la SSI en amont des projets.

Ces résultats exploratoires sont prometteurs pour aller vers une meilleure gouvernance SSI et une acculturation des dirigeants aux risques cyber. La mise en place d'un cyberscore semble pouvoir agir sur la perception SSI des dirigeants. Grâce à son design, les données exploitées et sa malléabilité, le CAM est un outil adaptable et appropriable à/par chaque organisation. Cependant, les critères retenus sont majoritairement techniques par soucis de rapidité d'implémentation mais la dimension organisationnelle devra être approfondie. Enfin, même si le comité a exprimé l'intention d'agir pour remédier au risque cyber, rien n'assure que de réelles actions vont être mises en place. La littérature a déjà prouvé qu'un utilisateur peut exprimer une intention d'agir pour sa cybersécurité, être sensibilisé à ce sujet, mais finalement ne réaliser aucune action sans que des raisons particulières n'aient été relevées (voir par exemple Acquisti & Grossklags, 2004). De ce fait, il serait intéressant d'étudier la mise en œuvre du cyberscore sur une plus longue période, ce qui permettrait de vérifier si de réelles actions ont été réalisées, au-delà de simples déclarations d'intention.

Aussi pertinent soit-il, le CAM ne doit toutefois pas s'appréhender comme un outil isolé. Il doit s'inscrire dans une gouvernance plus large du système de management de la sécurité de l'information d'une organisation (SMSI)[9]. À la fois dispositif d'alerte et outil d'aide à la décision, les critères identifiés à sa conception doivent nécessairement être couplés et intégrés à la politique globale de sécurité des systèmes d'information pilotée par la direction. De plus, et comme l'indique la Direction centrale de la sécurité des systèmes d'information, « *Il appartient au niveau décisionnel de prendre toute disposition pour concevoir et mettre en place une sécurité adaptée aux besoins et objectifs de l'organisme et de s'assurer du respect de l'application de la PSSI* » (2004, p.13). Enfin, il conviendra d'étudier (ou même de créer) les liens avec des dispositifs et méthodes existants comme la méthode d'analyse de risque EBIOS *Risk Manager*[10], soutenue par l'ANSSI et le Club de la sécurité de l'information français (CLUSIF[11]), et les travaux menés dans le cadre du maintien en condition du patrimoine (voir par exemple Brusselle et *al.*, 2021).

6. Discussion et perspectives

Accepter un risque ou non est un processus dépendant de la perception de ce risque pour un individu (Yates et Stone, 1992). Cependant, de nombreux biais cognitifs viennent perturber le jugement des individus (Tversky et Kahneman, 1973 ; Tversky, 1974 ; Slovic, 1979 ; Slovic, 1982 ; Tversky, 1981). En 1980, Slovic et ses collègues identifient même un écart de perception des risques entre les experts et les profanes (Slovic, 1980). Les profanes estiment que les experts

---

[9] Un « *SMSI se compose des politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par un organisme dans le but de protéger ses actifs informationnels. Un SMSI utilise une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métier* » (ISO/IEC 27000:2018, p.12).

[10] Présentation de la méthode EBIOS *Risk Manager* : https://bit.ly/3Qt3Alg (consulté le 4 décembre 2022).

[11] Site internet du CLUSIF : https://clusif.fr/.

minimisent les risques alors que, inversement, les experts expriment que le public a tendance à surestimer les risques. Nos travaux nous permettent de constater que cet écart expert / profane est inversé dans le cas du risque cyber. Il serait alors intéressant de chercher à identifier les biais de perception du risque propre au risque cyber en se basant, par exemple, sur deux modèles existants en SI : *Protection Motivation Theory* (PMT) (Rogers, 1975) et *Technology Threat Avoidance Theory* (TTAT) (Liang et *al*., 2010). Ces deux modèles de perception du risque SI mobilisent des méthodes quantitatives pour mesurer l'impact de facteurs cognitifs sur la perception. Ils laissent cependant peu de place aux dimensions organisationnelles de la perception du risque et ne se penchent pas encore sur la spécificité du risque cyber.

La littérature en perception des risques nous invite à étudier également direction générale dans le cadre de nos travaux de recherche en perception du risque cyber. Elle a en effet « *la responsabilité ultime de la sécurité. Toute action entreprise ou problème résolu doit être le résultat de l'intervention de la direction » (*Friend & Pagliari, 2000, p. 30). Reix et *al.* (2016) expliquent la nécessité d'une approche globale du risque SSI et de l'engagement de la Direction Générale : « pour les *responsables, la gestion de la sécurité se situe dans un univers incertain ; certains sinistres résultent de combinaisons difficilement envisageables de causes variées. [...] Ces difficultés justifient une approche globale du problème de la sécurité des SI »* (p. 443). Nos travaux se sont pour l'heure uniquement concentrés sur des dirigeants de premier niveau pour des raisons d'accessibilité. Cependant, Mintzberg (1994) explique qu'il existera toujours un décalage entre l'intention des dirigeants (au sens de la haute direction) dans la planification de leur stratégie et la stratégie réelle mise en place dans l'entreprise. Il évoque alors l'importance des cadres intermédiaires comme acteurs du changement. En effet, ces derniers sont les mieux placés pour réfléchir, agir et coordonner les actions visant à répondre à la stratégie d'entreprise et les revendications divergentes qui en découlent (Sharma et Good, 2003). Ainsi, ils sont des « *médiateurs importants entre les niveaux hiérarchiques et les unités opérationnelles » (*Wooldridge et *al.*, 2008, p. 1192). De plus en plus de recherches soulignent d'ailleurs leur importance pour gérer les divergences entre le sommet et les opérationnels (Huy, 2002) puisqu'ils ont un rôle important en tant qu'acteurs d'accompagnement du changement mais également en tant que destinataires du changement (Balogun, 2003). Il sera alors intéressant de ne pas négliger l'importance des cadres intermédiaires dans la poursuite de nos recherches en perception du risque cyber.

7. Conclusion

Dans cet article, nous avons cherché à construire un artefact en mesure d'agir sur a perception du risque cyber par la direction générale. Une revue de littérature a été réalisée en perception du risque nous permettant de confirmer un écart existant dans la perception du risque entre les experts et les profanes. Un éclairage sur les particularités du risque cyber nous a permis de constater que ce risque ne pouvait être approché comme les autres risques globaux en entreprise. Nous nous sommes alors concentrés sur la notion d'instrument de gestion permettant de venir décomplexifier la nature de ce risque et servant d'aide à la décision quant à son acceptabilité. À travers une approche de type DSR, nous avons construit un instrument de gestion nommé « cyberscore pour applicatifs métier » (CAM). Dans le cadre d'un mémoire de recherche appliquée du Master 2 Management de la Sécurité des systèmes d'information de l'IAE Paris-

Est, une première expérimentation a été menée au sein de la CASDEN Banque Populaire. Une note de D (sur un ensemble de note allant de A à E) sur une application métier vitale pour l'entreprise a été présentée en comité composé de dirigeants de premier niveau. Cette note et l'ensemble du projet ont ensuite été approfondis lors d'entretiens semi-directifs auprès de l'ensemble du comité. Les premiers résultats obtenus sont encourageants quant à la possibilité pour le CAM de venir agir sur la perception du risque des dirigeants de premier niveau. Une différence de perception est constatée avant et après présentation du prototype. Cependant, ces travaux ne permettent pas encore d'identifier les leviers permettant une meilleure perception du risque cyber chez un profil de dirigeant. De plus, même si la visée première de ces travaux était d'atteindre une population de type haute direction suite à la revue de littérature en perception des risques, la population de dirigeants intermédiaires semblent jouer un rôle important dans la mise en place réelle de la stratégie d'entreprise à ne pas négliger. C'est dans ce contexte passionnant et stimulant que nous débuterons une thèse CIFRE en 2023.

8. Références

Acquisti, A., Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1), 26-33.

Albrechtsen, E. (2007) A qualitative study of user's view on information security. Computer and Security 26 (4): 276–289.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.

Avolio, F.M. (2000). Best practices in network security: as the networking landscape changes, so must the policies that govern its use. Don't be afraid of imperfection when it comes to developing those for your group, *Network Computing*, 60(20), 60-72.

Balogun, J. (2003). From blaming the middle to harnessing its potential : creating change intermediairies. *British Journal of Management*, 14(1), 69-83.

Bandyopadhyay, K., Mykytyn, P. P., Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision*, 37(5), 437-445.

Barlette, Y. (2008). Une étude des comportements liés à la sécurité des systèmes d'information en PME. *Systèmes d'information & management*, 13, 7-30.

Barlette, Y. & Jaouen, A. (2019). Information security in SMEs: determinants of CEOs' protective and supportive behaviors. *Systèmes d'information & management*, 24, 7-40. https://doi.org/10.3917/sim.193.0007

Baskerville, R. (2008). What design science is not. *European Journal of Information Systems*, 17(5), 441-443.

Brusselle, C., Doré, A., Bonucci, L., Borg, L., Iori, M., Khanh, F., Ligneul, S. (2021). *Cybersécurité : méthode de gestion de crise*, VA-Éditions.

Direction centrale de la sécurité des systèmes d'information (2004). *Guide pour l'élaboration d'une politique de sécurité de système d'information – Section 3 Principes de sécurité*, Secrétariat général de la défense nationale.

Dhillon, G., Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.

Friend, M., Pagliari, L.R. (2000), « Establishing a safety culture: getting started », Professional Safety, 45(5), 30-32.

Goodhue, D.L., Straub, D.W. (1991). Security concerns of systems users: a study of perceptions of the adequacy of security measures, *Information and Management*, 20(1), 13-27.

Grover, V. (1993). Empirically derived model for the adoption of customer-based inter-organizational systems, *Decisions Sciences*, 24(3), 603-639.

Hevner, A., Chatterjee, S. (2010). *Design Research in Information Systems*. Springer-Verlag.

Hohenemser, C., R., Kates, W., Slovic, P. (1985). A casual taxonomy. Dans R. W. Kates, C. Hohenemser, & J. X. Kasperson (Eds.), *Perilous progress: Managing the hazards of technology*, 67–89. Boulder, Westview Press.

Huy, Q., (2002). Emotional balancing of organizational continuity and radical change : The contributions of middle managers. *Administrative Science Quarterly*, 47(1), 31-69.

International Organization for Standardization (2018). *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire* (ISO Standard No. 27000:2018).

Liang, H., Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

Loch, Carr, H., Warketin, M. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly*, 16(2), 173–186.

Peneloux, E. (2022), *Influencer la perception du risque de la sécurité des systèmes d'information : conception d'un cyberscore à destination de la direction*, Mémoire de recherche appliquée, Université Paris-Est Créteil.

McFadzean, E., Ezingeard, J. N., Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level, *Online Information Review*, 31(5), 622-660.

Mintzberg, H. (1994). *Grandeur et décadence de la planification stratégique*. Dunod.

Mishra, A. (2022). *Modern Cybersecurity Strategies for Entreprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods*. Bmp.

Netter, E. (2022). Un « cyberscore » pour les grandes plateformes et services de communication en ligne, *Revue trimestrielle de droit commercial et de droit économique*, 2, 309.

Ogbanufe, O., Kim, D. J. & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions : The role of institutional pressures, *Information & ; Management*, 58(7), 1-18.

Reix, R., Fallery, B., Kalika, M., Rowe, F. (2011). *Systèmes d'information et management des organisations, 6° édition.* Vuibert.

Reix, R., Fallery, B., Kalika, M., Rowe, F. (2016). *Systèmes d'information et management*. Vuibert.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology,* 91(1), 93-114.

Salamon, Y. (2020). *Cybersécurité, Cyberdéfense : enjeux stratégiques*. Ellipses.

Sharma, G., Good, D., (2013). The Work of Middle Managers : Sensemaking and Sensegiving for creating Positive Social Change. *Journal of Applied Behavioral Science*, 49(1), 95-122.

Simon, H. (2004). *Les sciences de l'artificiel*. Éditions Gallimard.

Sjöberg, L., Moen, B. E., & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm, *Norwegian University of Science and Technology*, C Rotunde Publikasjoner.

Slovic, P. Fischhoff, B., Lichtenstein, S. (1979). *Rating the risks. Environment*, 2(3). 14-20 et 36-39.

Slovic, P. Fischhoff, B., Lichtenstein, S. (1980). *Facts and fears :* understanding perceived risk. *In :* Schwing, R., Albers, W., *Societal risk assessment.* Plenum Press, New York, 1881-214.

Slovic, P. Fischhoff, B., Lichtenstein, S. (1982). Psychological aspects of risk perception. *In :* Sills, D., Wolf, C., Shelanski, V. *The accident at Three Mile Island: the human dimensions.* Westview Press, Boulder, 11-19.

Slovic, P. (1987). Perception of risk, *Science*, 236(4799), 280-285.

Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. *Risk analysis*, 29(4), 689-701.

Straub, D., Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), 441-469.

Taylor, R. (2006). Management perception of unintentional information security risks. *ICIS 2006 Proceedings*.

Tsohou, Karyda, M., Kokolakis, S., Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security*, 14(3), 198–217.

Tversky A., Kahneman, D. (1973). Availability: a heuristic for judgind frequency and probability. *Cognitive psychology,* 5 : 207-232.

Tversky A., Kahneman, D. (1974). Judgment under incertainty: heuristics and biaises. *Science,* 185(4157), 1124-1131.

Tversky A., Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science,* 211(4481), 453-458.

Wooldridge, B., Schmidt, T., Floyd, S.W., (2008). The middle management perspective on strategy process : contributions, synthesis, and future research. *Journal of Management*, 34(6), 1190-1221.

World Economic Forum, 2012. *Global risks 2012. Seventh edition, Insight Report*, Geneva.

Yates, J. F., Stone, E. R. (1992). *The risk construct*. John Wiley & Sons.