Farjaudon, Anne-Laure; Gardès, Nathalie

Article

La maturité cyber au prisme de la communication extra-financière : une analyse des entreprises du CAC 40 = Cyber maturity through the prism of extra-financial communication

Revue française de gestion industrielle

Reference: Farjaudon, Anne-Laure/Gardès, Nathalie (2024). La maturité cyber au prisme de la communication extra-financière : une analyse des entreprises du CAC 40 = Cyber maturity through the prism of extra-financial communication. In: Revue française de gestion industrielle 38 (2), S. 67 - 85.
https://rfgi.fr/rfgi/article/download/1187/1638/2832.
doi:10.53102/2024.38.02.1187.

2024, Vol. 38, No. 2, 67-85

Revue Française de Gestion Industrielle

article en open accès sur www.rfgi.fr

https://doi.org/10.53102/2024.38. 02.1187

ISSN: 0242-9780
eISSN: 2804-9284

La maturité cyber au prisme de la communication extra-financière : une analyse des entreprises du CAC 40

Anne-Laure Farjaudon[1], Nathalie Gardès[2]

[1] *Univ. Bordeaux, IRGO, EA 4190, F-33000 Bordeaux, France, anne-laure.farjaudon@u-bordeaux.fr*

[2] *Univ. Bordeaux, IRGO, EA 4190, F-33000 Bordeaux, France, nathalie.gardes@u-bordeaux.fr*

Résumé : L'objectif de ce papier est d'analyser le contenu des informations diffusées par les entreprises pour en déduire leur niveau de maturité en cas de cyberattaques. La survie d'une organisation ne dépend pas uniquement d'actions relatives à la cybersécurité, mais bien de sa capacité à récupérer et apprendre et donc à être résiliente. La résilience d'une organisation face à un risque cyber intéresse donc au plus haut point les parties prenantes. Si la communication extra-financière est un sujet qui préoccupe les chercheurs depuis longtemps, rares sont les articles qui s'intéressent à la communication en matière de risques cyber. L'objectif de cette étude est de caractériser la communication des grandes entreprises en la matière, notamment en identifiant la nature des informations publiées dans les rapports annuels et leur degré de précision. L'analyse des pratiques de diffusion de l'information nous permet de caractériser le degré de cyber résilience des entreprises du CAC 40.

Mots clés : cybersécurité ; cyber résilience ; informations extra-financières ; risques ; rapports annuels

Cyber maturity through the prism of extra-financial communication: an analysis of CAC 40 companies

Abstract: The aim of this paper is to analyze the content of information disseminated by companies in order to deduce their level of maturity in the event of cyber-attacks. An organization's survival does not depend solely on cybersecurity actions, but on its ability to recover and learn, and thus to be resilient. An organization's resilience in the face of cyber risk is therefore of the utmost interest to its stakeholders. While extra-financial communication has long been a subject of concern to researchers, few articles have focused on cyber risk communication. The aim of this study is to characterize the communication of major companies in this area, in particular by identifying the nature of the information published in annual reports and their degree of precision. Our analysis of information dissemination practices enables us to characterize the degree of cyber resilience of CAC 40 companies.

Keywords: cybersecurity, cyber resilience, extra-financial information, risks, annual reports

---

Citation : Farjaudon, A-L. & Gardès, N. (2024). La maturité cyber au prisme de la communication extra-financière : une analyse des entreprises du CAC 40. *Revue Française de Gestion Industrielle*, 38(2), 67-85. https://doi.org/10.53102/2024.38. 02.1187

Historique : reçu le 03/07/2023, accepté le 15/03/2024, en ligne le 30/04/2024

1. INTRODUCTION

La cybersécurité constitue un enjeu majeur pour les organisations, quelles que soient leur taille ou leur secteur d'activité. Selon le baromètre annuel du CESIN 2024[1] (Club des Experts de la Sécurité de l'Information et du Numérique) 49% des entreprises sondées déclarent avoir subi au moins une cyberattaque ayant un impact significatif. Ceci est d'autant plus inquiétant que la littérature fait état pour l'entreprise de pertes et coûts financiers directs et indirects importants pouvant compromettre la survie de l'organisation (Wang et Park, 2017). Avec le déploiement massif des activités à distance (suite à la pandémie du covid 19) et un contexte international tendu (cyberguerre), les possibilités d'attaque sont plus nombreuses. La prise en compte de cette menace par les entreprises est aujourd'hui un incontournable, et les défis de la cybersécurité deviennent une priorité pour nombre d'entre elles.

Le terme de cybersécurité ne fait pas l'objet d'un consensus dans la littérature académique (Craigen et al., 2014). Certaines définitions s'attachent à présenter la cybersécurité comme des méthodes défensives visant la détection des attaques (Kemmerer, 2003), la protection des réseaux informatiques et des informations (Lewis, 2006) et plus globalement comme un ensemble d'approches de gestion des risques d'intrusion malveillante (Amoroso, 2006 cité par Craigen et al. 2014). Selon Arpagian (2018), « la cybersécurité porte aussi bien sur la protection et l'attaque d'équipements informatiques (la guerre pour ou contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la toile (la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement ». La cybersécurité adopte ainsi une approche principalement technique et statique, axée sur les technologies de l'information visant à établir un périmètre de sécurité autour des ressources numériques pour les protéger contre les menaces.

De fait, les questions relatives à la gouvernance d'entreprise ainsi que les processus mis en place par les organisations pour maîtriser les risques cyber sont aujourd'hui au centre des réflexions car se jouent la confiance des parties prenantes et la survie de l'entreprise. Les répercussions d'une attaque sont en effet loin d'être anodines pour les clients (perte ou captation de leurs données) ou les financeurs (la mise en péril de l'entreprise peut compromettre sa capacité à honorer ses engagements). C'est la raison pour laquelle les entreprises ont aujourd'hui un devoir d'information auprès de leurs parties prenantes en termes de risques et violations possibles en matière de cybersécurité et des contre-mesures pertinentes mises en œuvre pour atténuer ces risques (Cheong et al., 2021). Il est de plus de l'intérêt des entreprises d'assurer une communication sur le sujet, attendu que le degré de protection de l'entreprise est aujourd'hui une condition de son financement et que la diffusion d'informations relatives à la cybersécurité se traduit par une appréciation positive par les marchés financiers (Berkman et al., 2018).

Toutefois, en dépit des multiples mesures de sécurité déployées, il reste une possibilité non négligeable qu'une cybermenace réussisse à contourner les protections mises en place, en touchant tout ou partie de l'entreprise, notamment la *supply-chain* (Derrouiche, 2022). L'augmentation de la sophistication, de la fréquence et de l'intensité des cyberattaques ciblant tant les entreprises que les institutions publiques illustre leur caractère incontournable ainsi que la difficulté technique à préserver intégralement la sécurité des infrastructures informatiques essentielles. Dans ce cadre, adopter une stratégie de cyber-résilience se présente comme une option pertinente, marquant un tournant par rapport à l'approche traditionnelle en matière de cybersécurité (Dupont et al., 2023). De ce fait, être prêt à réagir face à une attaque et à restaurer les fonctions vitales de l'entreprise s'avère crucial pour le maintien de son activité. L'accent est ainsi mis sur une nécessaire augmentation de la cyber-résilience c'est-à-dire la capacité d'une organisation à continuer de fonctionner malgré une

[1] https://cesin.fr/document.php?d=65b75aaa4ec50

attaque ou une menace cyber, et à se rétablir rapidement après un incident. D'après Dupont et al. (2023), la cyber-résilience diffère donc de la cybersécurité qui se concentre uniquement sur la capacité d'une organisation à prédire, prévenir et éviter l'apparition de cyber-risques (mise en place de barrières, de défenses et de protocoles pour empêcher les incidents). La cyber-résilience s'inscrit donc dans une perspective plus large en examinant comment les cyber risques qui peuvent menacer la survie de l'organisation ont un impact sur une gamme variée de processus opérationnels (Björk et al., 2015). L'objectif visé est de permettre à l'organisation de maintenir la continuité de ses fonctions ou services essentiels et de conserver la confiance de ses parties prenantes (Björk et al., 2015).

Afin de maintenir cette confiance, l'entreprise devra donc communiquer sur les moyens et actions mis en place pour assurer non seulement sa cybersécurité mais aussi sa cyber résilience. La communication extra-financière est un sujet qui préoccupe les chercheurs depuis longtemps (dès 1973, selon Erkens et al., 2015), notamment sur la RSE. Or, cette littérature sur le reporting extra-financier semble négliger le risque cyber alors même qu'il s'agit d'informations extra-financières faisant l'objet d'une diffusion volontaire de la part des entreprises. Rares sont les articles qui s'intéressent à la communication en matière de risques cyber. Cette littérature porte sur différentes thématiques : le contexte spécifique d'une cyberattaque ; la communication de crise pour minimiser l'impact en termes de réputation et de performance (Gao et al. 2020 ; Lehu, 2018 ; Wang et Park, 2017) et les bonnes pratiques à adopter (Zhang et Borden, 2020) ; le type d'informations communiqués dans les rapports d'activités (Bahl et al., 2020 ; Fortin et Héroux, 2020, Nurse et al. 2011) et enfin les réactions du marché à la suite d'une cyberattaque (Li et al., 2018 ; Gordon et al., 2011). A notre connaissance aucune étude ne s'est penchée sur le type d'information communiqué dans les rapports d'activité des entreprises du CAC 40 au-delà des seuls outils techniques déployés.

L'objectif de cet article est donc de répondre à la question de recherche suivante : comment les grandes entreprises communiquent-elles sur les risques cyber ? Notre intention est d'analyser à travers les rapports annuels le niveau de maturité cyber d'une organisation, entendu comme sa capacité à adopter les meilleures pratiques, se conformer aux normes, gérer de façon proactive son profil de risque (niveau de préparation humain, organisationnel et technique), apprendre et se remettre d'une attaque. Notre démarche vise donc à évaluer leur niveau de préparation face à une cyberattaque, leur robustesse dans la préservation de leurs activités malgré les cybermenaces, ainsi que leur agilité à retrouver un fonctionnement optimal après un incident, en soulignant l'importance des mécanismes proactifs et réactifs qu'elles mettent en place, afin d'en déduire leur niveau de maturité. Nous cherchons enfin à identifier s'il existe des groupes similaires sur leurs pratiques.

Nous contribuons à la littérature sur différents points : sur la communication extra financière, notre travail met en évidence la nécessité d'une structuration des informations relatives aux risques cyber, voire d'une normalisation des pratiques, comme c'est le cas pour la RSE. Nous apportons également plusieurs contributions à la littérature existante en matière de divulgation et de pratique de communication d'information relative aux risques cyber. Cette étude nous permet de caractériser la communication des grandes entreprises en matière de cyber résilience dans leur rapport d'activité, notamment en identifiant la nature des informations publiées dans les rapports annuels et leur degré de précision.

Notre propos s'articule autour de trois parties. La section 2 présente une revue approfondie de la littérature afin de clarifier le concept de cyber résilience. Notre objectif est d'appréhender leurs implications multiformes auprès des différentes parties prenantes et de caractériser les enjeux primordiaux ainsi que la posture stratégique adoptée par les entreprises à cet égard. La section 3 détaille la méthodologie mise en œuvre pour décortiquer les stratégies communicationnelles en matière de risques cyber par les entreprises du CAC 40. En arrière-plan, notre ambition est d'évaluer si les entreprises, identifiées comme étant

particulièrement exposées aux risques cyber, démontrent une résilience et une préparation proportionnées face à ces menaces. La section 4 expose et discute nos résultats.

2. COMMUNIQUER SUR LA CYBER RESILIENCE : UN ENJEU MAJEUR POUR LES ENTREPRISES

Compte tenu des impacts potentiels d'une cyberattaque sur les parties prenantes, la capacité d'une entreprise à communiquer sur sa cyber résilience est un enjeu majeur (Dupont et al., 2023).

2.1. La cyber résilience : un facteur clé de la confiance des parties prenantes

- Les cyberattaques, des impacts importants pour l'entreprise et ses parties prenantes

Aujourd'hui le risque cyber est devenu un sujet incontournable pour les entreprises et les gouvernements en raison de la fréquence accrue des cyberattaques et des coûts induits. De tels risques peuvent menacer la survie de l'ensemble de l'organisation en raison des impacts sur une gamme variée de processus opérationnels (Björk et al., 2015). Définie comme "une action individuelle ou collective délibérée, qui vise à porter atteinte à l'intégrité du système d'information informatisé d'une personne, d'une entreprise, d'une organisation ou d'un État, à l'aide de tout ou partie du réseau Internet (ou de tout autre réseau cybernétique)" (Lehu, 2018), les cyberattaques peuvent être catégorisées selon quatre types : les violations de données (divulgation non autorisée d'informations personnelles), les incidents de sécurité (attaques malveillantes dirigées contre une entreprise), les violations de la vie privée (violation présumée de la vie privée des consommateurs) et les incidents de phishing/skimming (crimes financiers individuels) (Romanosky, 2016).

La littérature fait état de différents coûts et pertes pour l'entreprise et ses parties prenantes (clients, fournisseurs, actionnaires, investisseurs). Pour les clients ou salariés, les préjudices d'une perte de données sont liés à l'utilisation malveillante de son identité et ses données. Pour l'investisseur, une cyberattaque touchant un client de son portefeuille a pour conséquence d'accroître le risque et donc la rentabilité de son investissement. Pour l'entreprise, la littérature distingue généralement les impacts en deux catégories, directes et indirectes (Eddé, 2020 ; Douzet et Héon, 2013).

Les pertes financières directes pour l'entreprise ou ses actionnaires proviennent d'un arrêt d'activités, d'une désorganisation de l'entreprise qui induit, d'une part la dégradation de l'efficacité des systèmes et processus internes et d'autre part, l'insatisfaction des clients (Eling et Wirfs, 2019 ; De Mereuil et Bonnefous, 2016). Les pertes indirectes se rapportent généralement à des pertes de données (données stratégiques sur les produits), vols de données (de salariés, de clients ou de fournisseurs), atteinte à l'image de marque (Whitler et Farris, 2017) et à la réputation de l'entreprise auprès des investisseurs, clients et opinion publique (Ben Jabeur et Serret, 2019 ; Kamiya et al., 2021). Ces pertes peuvent également être la conséquence d'une dégradation de la confiance des partenaires d'affaires, fournisseurs, investisseurs et clients (perte pouvant atteindre 4,5% des clients existants suite à une cyberattaque et jusqu'à 45% de perte de clients dans le secteur des assurances, voir une perte d'éventuels futurs clients). D'autres auteurs ont identifié des pertes liées à la dévaluation de la valeur d'une marque, à la baisse de la valorisation de l'entreprise (Romanosky, 2016 ; De Coste, 2017) et à l'impact sur le cours de l'action (Kamiya et al. 2021, Hilary et al. 2016). Les coûts financiers directs sont relatifs aux coûts du nettoyage de l'attaque (Douzet et Héon, 2013), aux coûts de reconstruction et de sécurisation du système d'information, aux coûts de communication (interne et externe auprès des parties prenantes) et aux coûts juridiques (Romanosky, 2016). Ils concernent également les frais de gestion de crise liés à la mobilisation spécifique des collaborateurs ou d'experts externes, l'achat de matériels ou logiciels, et la mise en place d'une communication de crise (Wang et Park, 2017 ; Lehu, 2018). Ces coûts peuvent également être générés par une rupture contractuelle des engagements de la société impliquant des pénalités ou amendes réglementaires pour non-respect de ceux-ci.

Les coûts indirects proviennent d'une augmentation possible du coût de la dette et des primes d'assurance, de la perte de propriété intellectuelle ou de données sensibles (secret de fabrication). Ils peuvent également découler de la défiance des investisseurs et fournisseurs (Anderson et al. 2012 ; Kamiya et al., 2021 ; Gao, 2020) qui menace la survie de l'entreprise. En effet, les investisseurs et repreneurs tiennent compte des risques cyber dans l'évaluation des entreprises qu'ils convoitent. Enfin, Ben Jabeur et Serret (2019) citent les coûts intangibles exceptionnels du licenciement du PDG.

L'estimation financière précise des conséquences d'une cyberattaque est toutefois difficile en raison de la temporalité des effets (immédiats et différés), mais également parce que les coûts et pertes peuvent être cachés ou inconnus. Par exemple, la frustration des clients ou l'atteinte à la réputation (Tariq, 2018), les effets sur l'innovation des entreprises (He, Frost et Pinsker, 2019) ou encore l'accroissement des frais d'audit (Li, No et Boritz, 2020) ne sont pas toujours directement mesurables.

Face à l'ampleur des pertes et coûts potentiels, on comprend que les cyberattaques soient en mesure de mettre en péril l'entreprise (Wang et Park., 2017). Par conséquent, si l'enjeu est la survie, les entreprises vont devoir penser non seulement à leur cybersécurité mais également à leur cyber résilience. En effet la cybersécurité s'intéresse à la protection des systèmes. On peut la définir comme l'organisation et l'ensemble des ressources, processus et structures utilisés pour protéger le cyberespace et les systèmes basés sur le cyberespace contre des attaques, accès illégaux, modification ou destruction (Craigen et al 2014 ; Kruse et al., 2017). Toutefois aucun système n'étant infaillible l'entreprise doit être en mesure pour survivre d'être cyber-résiliente i.e. la capacité des cyber-systèmes à s'adapter et à rebondir après les effets d'une attaque.

Nous allons dans ce qui suit nous intéresser au concept de résilience afin de bien distinguer les concepts de cyber sécurité et cyber résilience.

- De la résilience à la cyber-résilience

La résilience organisationnelle décrit la compétence et la capacité de l'organisation à s'adapter à des environnements de risque dynamiques et divers. Une organisation résiliente est donc capable de changer et de s'adapter avant que son environnement ne la force à le faire (Hamel et Valinkangas, 2003). La littérature portant sur la résilience permet d'identifier deux conceptions de ce concept.

La première, qualifiée de passive (Yilmaz Borekci et al., 2015), d'adaptative (Orchiston et al., 2016), de douce (Proag, 2014) ou de faible (Altintas et Royer, 2009) traduit l'aptitude d'une organisation à absorber un choc sans transformation des fonctions ou structures organisationnelles. Par exemple, la couverture d'une assurance contre les pertes dues aux cyberattaques s'inscrit dans cette vision. Ce type de stratégie comporte des lacunes. En effet, l'assurance ne couvre que l'indemnisation financière sans pour autant gérer les externalités négatives comme l'impact sur la réputation. En outre, la souscription d'une assurance ne constitue pas une capacité organisationnelle, puisqu'elle ne réduit pas la probabilité qu'une cyberattaque se reproduise.

La seconde, dite active, dure (Proag, 2014), stratégique (Hamel et Valinkangas, 2003) ou forte (Altintas et Royer, 2009) se caractérise par le déploiement d'activités proactives afin d'éviter des situations de crise (Hamel et Valinkangas, 2003 ; Roux-Dufort, 2003) ou l'effondrement de l'organisation (Proag, 2014) en cas de choc. Elle inclut le développement de nouvelles options comme la mise en place de procédures spécifiques en cas d'attaques (Wang et Park, 2017) qui permettent à l'entreprise de ne pas s'effondrer face à l'inattendu ou au choc. Cette capacité d'absorption (Weick et Sutcliffe, 2011) assure à l'entreprise d'être en mesure de pouvoir agir (plan d'action, circulation de l'information). Elle implique également une capacité d'appropriation permettant à l'entreprise de devenir plus forte en capitalisant sur ses expériences (Weick et Sutcliffe, 2011 ; Altintas, 2020) ce qui suppose de transformer l'entreprise en système apprenant.

La résilience organisationnelle est ainsi le résultat de la résilience des fonctions ou processus stratégiques et opérationnels essentiels de l'organisation, de la planification stratégique à la gestion de la chaîne d'approvisionnement, en passant par les opérations informatiques, la gestion de la sécurité et la gestion financière. Un manque de résilience dans l'une de ces fonctions ou processus essentiels affecte directement la résilience globale de l'organisation. A l'ère numérique la cybersécurité et la cyber résilience sont clés dans la résilience d'une organisation.

Selon Linkov et Kott (2019), la cyber résilience désigne la capacité d'un système à se préparer, absorber, récupérer et s'adapter aux impacts négatifs, particulièrement ceux résultant des cyberattaques. Cette définition met en lumière la nature dynamique et holistique de la cyber résilience, soulignant l'importance de la préparation, la capacité de réponse et de récupération face aux cyber menaces. Sa portée s'étend au-delà de la simple prévention d'attaques. Sepúlveda-Estay et al. (2020) précisent qu'elle comprend également la capacité de réaction organisationnelle pour réduire les interruptions lors des incidents, suggérant une approche proactive de la gestion des risques et une faculté d'adaptation pour surmonter les attaques. Son objectif ultime est donc d'assurer que l'organisation puisse continuer à offrir ses services ou fonctions essentiels, même en cas de cyberattaque (Björk et al., 2015). Cela implique une construction multidisciplinaire et transversale de la résilience, nécessitant une collaboration entre différents acteurs de l'organisation ainsi qu'avec des organisations partenaires (Björck et al., 2015, Craigen et al., 2014) qui oblige à relever des défis organisationnels (processus, méthodes, gouvernance), humains (sensibilisation, engagement formation), technologiques (solutions logicielles), économiques (investissements) mais également politique (Goodall et al., 2009 ; Deibert et Rohozinski, 2010).

Dupont et al. (2023) précisent que « la cyber-résilience reflète une perspective plus large qui consiste à examiner comment les cyber-risques qui peuvent menacer la survie de l'ensemble de l'organisation ont un impact sur une gamme variée de processus opérationnels ». Cela nécessite une compréhension approfondie des cyber-risques, de leur incidence sur les activités opérationnelles et de la pérennité de l'organisation.

Le tableau 1 ci-dessous présente les principales différences entre la cybersécurité et la cyber-résilience :

Tableau 1: Différences entre cybersécurité et cyber-résilience (à partir de Dupont et al. (2024))

	Cybersécurité	Cyber-résilience
Objectifs	Préparer et protéger les systèmes informatiques contre une attaque	Préparer, prévenir, protéger, répondre, absorber, récupérer et s'adapter face à une attaque
Approche	Proactive et technique	Proactive, réactive et holistique
Champ d' application	Perception principalement restreinte aux technologies de l'information	Perception élargie en étudiant l'organisation dans son ensemble (technique, organisationnel, social et économique)
Horizon	Court terme	Long terme

Compte tenu des répercussions d'une cyberattaque sur les différentes parties prenantes, ces dernières vont chercher à mesurer la cyber résilience des organisations, c'est à dire, s'intéresser à leur capacité à contenir, minimiser l'ampleur des perturbations causées par une cyberattaque et reprendre rapidement leurs niveaux de performance rapidement et efficacement (Dupont et al., 2023). L'entreprise doit faire en sorte d'être transparente dans sa communication sur les actions mises en place afin de rassurer et de créer de la confiance auprès de l'ensemble de ses parties prenantes, notamment des investisseurs en témoignant de sa capacité à se protéger et prévenir le risque en amont, réagir en cas d'attaque, se réparer et se remettre d'une attaque.

2.2. La communication cyber : une mesure indirecte de la maturité cyber

Compte tenu des impacts d'une cyberattaque sur les parties prenantes, ces dernières vont chercher à évaluer le degré de maturité cyber des organisations (Kamiya et al. 2021).

- Les modèles de maturité cyber

La maturité cyber fait référence à l'évaluation de l'état de préparation et de récupération de l'organisation par rapport à différents critères (Bahuguna et al., 2019). Il existe plusieurs modèles de maturité cyber, notamment le modèle C2M2 (Cybersecurity Ccapability Maturity Model) de Curtis et al. (2015), le modèle du management de la résilience de Caralli (2006) et de Caralli et al. (2010) et le modèle de maturité de la cybersécurité communautaire (CCSMM) de White (2011). D'une manière générale, tous les modèles de maturité cyber partagent un objectif fondamental : offrir un cadre de référence qui permet aux entités d'évaluer leurs pratiques actuelles, d'identifier leurs faiblesses et d'établir des priorités pour une amélioration continue. C'est donc un outil d'auto-évaluation qui sert également de feuille de route pour guider le développement des processus.

Toutefois ces modèles se distinguent par le degré d'étendue ou l'ampleur de la gestion des risques cyber. Le modèle C2M2 se focalise sur la gestion des risques, notamment par l'établissement de plans rigoureux et de procédures adaptées pour gérer les vulnérabilités. La culture de la cybersécurité y est également mise en exergue, signifiant que la sécurité ne dépend pas uniquement des technologies, mais aussi de l'attitude et des connaissances des personnes impliquées. Quant au CCSMM de White (2011), il s'efforce de cartographier l'évolution de la maturité cyber, débutant par la simple sensibilisation, avant de culminer vers des méthodes techniques et pratiques avancées. Ces deux modèles cherchent avant tout à améliorer la posture de cybersécurité des organisations, ils proposent des méthodes et des domaines d'accentuation différents pour atteindre cet objectif.

Le modèle de management de la résilience de Caralli (2006), en revanche, est beaucoup plus large puisqu'il se centre sur six éléments essentiels du management de la résilience opérationnelle. La singularité de ce modèle est sa capacité à envisager la continuité du service, la collaboration avec des partenaires externes, et la garantie d'opérations informatiques ininterrompues, même en cas de cyberattaques.

L'un des principaux défis associés à l'étude de la cyber-résilience réside dans le fait qu'elle doit couvrir un grand nombre de dimensions : technique, organisationnelle et humaine. Elle s'intéresse à l'efficacité des processus de gestion des risques cyber aux différentes étapes qui composent le cycle de la cyber-résilience (préparer, prévenir, protéger, répondre, récupérer, s'adapter) (Häring et al., 2016). Son évaluation nécessite donc de prendre en compte de multiples critères que nous allons détailler dans la section suivante.

- Vers la constitution d'une grille d'évaluation

Évaluer la maturité cyber entendue comme non seulement la préparation à une attaque (cybersécurité) mais également la continuité et récupération (cyber-résilience) est complexe. Il s'agit en effet d'analyser les pratiques à différentes étapes du cycle de vie du risque (Keys et Shapiro, 2019). La plupart des cadres se concentrent sur la gestion des connaissances avant l'événement (analyse des risques et activités de prise de conscience) et sur les mesures opérationnelles (sécurité, visibilité des systèmes, rapidité de réaction) (Sepúlveda Estay et al., 2020).

Pour élaborer une grille d'analyse (Tableau 2), nous nous sommes appuyées sur les travaux de Bahuguna et al. (2019), Curtis et. al. (2015), White et. al. (2011), Héroux et Fortin (2020), Caralli (2006) et Caralli et al. (2010) ainsi que sur les différentes dimensions établies par l'AMF (Autorité des Marchés Financiers). Les thématiques dites SPOT (Supervision des Pratiques Opérationnelle et Thématique[2]), recouvrent les points suivants : l'organisation des dispositifs de cybersécurité en matière de moyens humains et techniques ; la gouvernance de ces dispositifs ; les dispositifs d'administration et de surveillance du système d'information ; le processus de gestion des incidents cyber ; la gestion des données sensibles ; le plan de

[2] https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-publie-la-synthese-de-ses-controles-thematiques-sur-les-dispositifs-de-cybersecurite-en-place

continuité d'activité ; le contrôle interne en place sur le système d'information et sur le dispositif de cybersécurité.

Tableau 2 : Grille d'analyse cyber résilience

QUALIFICATION / IMPACT
Gestion Risque de cybersécurité / description des risques
Défis rencontrés / Impacts potentiels d'un incident cyber
GOUVERNANCE : RESPONSABILITÉ
Équipe de réponse aux incidents
Groupe responsable identifié pour la mise en œuvre de la politique de cybersécurité
Constitution d'un comité de gestion des cyber-crises
Audits/évaluations de la cybersécurité
PROCESS : GESTION DES MENACES ET DES VULNÉRABILITÉS
Plan de gestion de crise cybernétique (PGCC) ou plan de réponse aux incidents (PRI)
Plan de continuité de service
Gestion de programme / politique de cybersécurité
Normes ou cadres de cybersécurité ISO
Gestion des identités et des accès
PROCESS : PLANS DE REPRISE
Plan de reprise/réponse en cas de catastrophe/ incident
Plan de continuité de service
Réponse aux événements et aux incidents
ATTÉNUATION DU RISQUE / RENFORCEMENT DES CAPACITÉS
Programme de formation et de sensibilisation des employés à la cybersécurité
Détecter et répondre aux attaques : identifier, analyser, gérer les menaces
Allocation d'un budget pour la cybersécurité
Assurance
Participation à des exercices de cybersécurité : test d'intrusion / test du plan de reprise
Ajustements à partir d'attaques précédentes
Mécanisme en place pour l'application/le respect de la loi (RGPD)
Gestion de la chaîne d'approvisionnement et des dépendances externes

S'il devient urgent que les questions de cybersécurité et cyber-résilience fassent dorénavant partie intégrante des dispositifs de communication des entreprises, et pas seulement lorsque la crise éclate, la question des informations à divulguer se pose : quelles informations divulguer et comment (quel support) ?

Compte tenu de l'attention portée à la cyber-résilience, au regard de leurs impacts et de l'intérêt porté par les parties prenantes, il est nécessaire de comprendre comment bien communiquer. Une absence de communication sur la gestion du risque cyber témoigne a priori d'une faible maturité dans la gestion de ce risque et pourrait entraîner une perte de confiance envers l'entreprise. L'enjeu d'une bonne communication est de faciliter la compréhension des risques, leur maîtrise par les entreprises afin de divulguer aux parties prenantes leur niveau de gestion des risques et favoriser un jugement favorable (Nurse et al., 2011).

La communication des risques a fait l'objet de nombreuses recherches notamment dans les domaines de la santé et des catastrophes naturelles. On peut la définir comme le processus interactif d'échange d'informations sur un risque (sa nature, sa signification, ses conséquences, sa probabilité et les options de réponse) avec les individus, afin qu'ils puissent porter un jugement en connaissance de cause. Toutefois, peu d'articles ont traité de la communication ou des pratiques de divulgation des impacts des risques en matière de risques cyber (Héroux et Fortin, 2020).

Or, communiquer sur un risque suppose de communiquer des informations pertinentes et informationnelles. Si les modèles de résilience nous donnent des éléments de contenu, se pose la question du support pour que celles-ci puissent être perçues comme fiables, de qualité et utiles (Cheong et al., 2021 ; Gao et al., 2020). En effet, la qualité d'une information est liée à sa valeur informative et la confiance qu'elle est susceptible de générer pour l'individu qui la reçoit. Il est donc essentiel de comprendre les aspects qui influencent la perception de la fiabilité de l'information pour atteindre l'objectif d'une communication des risques digne de confiance et efficace. Parmi les

différents leviers de communication dont elle dispose, le rapport d'activité constitue un support traditionnel, digne de confiance, et supposé exhaustif en matière de divulgation des informations financières et non financières aux différentes parties prenantes (Senkel, 2009). Son caractère officiel lui confère une légitimité et permet une comparaison entre différentes organisations sur la nature et le degré de précision des informations extra-financières communiquées. La communication via les rapports annuels constitue en effet le moyen privilégié pour exposer les actions mises en place (Eijkelenboom et Nieuwesteeg, 2021). Le rapport annuel permet en effet de communiquer des informations pertinentes, complètes, dignes de confiance et accessibles à l'ensemble de ses parties prenantes.

Le support de communication étant défini, la question est alors celle des informations nécessaires à une bonne compréhension de la manière dont les organisations se préparent aux cyber chocs, les absorbent, y répondent et s'en remettent (Grøtan et al., 2022).

Evaluer la maturité cyber nécessite de communiquer des informations sur (cf. grille d'analyse) :

1) La préparation et la prévention (formation, sensibilisation du personnel, crash-test, système de détection, cartographie des risque),
2) La protection (comment l'entreprise empêche la réalisation d'un risque cyber pour un service de grande valeur : identification des menace),
3) Les réponses de l'organisation en cas de menace (maintenir un service de grande valeur si le risque est réalisé, plan de reprise d'activité ou de continuité),
4) La récupération (traiter efficacement les conséquences pour l'organisation si le risque est réalisé, et rendre l'organisation à un état opérationnel « normal »,
5) Adaptation (comment l'entreprise s'est adaptée et a appris à la suite d'une attaque).

Ces informations peuvent être plus ou moins sensibles voire stratégiques, se pose donc la question du juste niveau de divulgation de celles-ci. Selon Hilary et al. (2016), une divulgation excessive peut être contre-productive. En effet, "la divulgation complète accélère la diffusion des attaques, augmente la pénétration des attaques au sein de la population cible et accroît le risque de première attaque après le signalement de la vulnérabilité" (Mitra et Ransbotham, 2015). Les diffusions détaillées peuvent ainsi fournir « une feuille de route aux attaquants » des faiblesses de l'entreprise (Li et al., 2018).

Ainsi, si les actionnaires et les investisseurs ont besoin d'informations sur le risque cyber pour guider leurs décisions d'investissement (Bakker et Streff, 2016), les dirigeants doivent faire attention à la portée de la divulgation du risque cyber afin de protéger les intérêts de leur organisation. Compte tenu de la tension entre ces besoins contradictoires, il est difficile de définir un niveau optimal de divulgation du risque cyber. On notera d'ailleurs que les entreprises adoptent des comportements stratégiques dans la gestion de cette divulgation (Cheong et al., 2021). Les entreprises victimes d'atteinte à la sécurité informatique ne fournissent généralement pas suffisamment d'informations après avoir subi une attaque (Cheong et al., 2021) et ont tendance à ne pas diffuser les informations négatives dès lors que les parties prenantes (investisseurs) n'ont pas la capacité de les identifier. En revanche, si la probabilité de découvrir l'attaque est forte, l'entreprise a intérêt à être transparente. En effet, la perte de la valeur de l'action sera moins importante si l'entreprise a communiqué (baisse de 3,6% contre 0,7%) que si elle a volontairement caché l'attaque (Amir et al., 2018). De telles pratiques conduisent à réduire le caractère informatif des divulgations en rendant plus flou la vulnérabilité de l'entreprise (Cheong et al., 2021).

Ces comportements stratégiques peuvent cependant être contreproductifs à l'échelle collective. En effet, d'un point de vue collectif, le partage de l'information sur les cyberattaques présente deux types d'avantages : (1) une plus forte résistance aux cyberattaques (2) une réduction des coûts d'investissement dans la sécurité (Pala et Zhuang, 2019).

3. METHODOLOGIE DE LA RECHERCHE

Conformément à Héroux et Fortin (2020) et Eijkelenboom et Nieuwesteeg (2021), nous avons utilisé les rapports annuels comme support privilégié de divulgation d'informations sur le risque cyber. En effet, si la communication d'une entreprise peut se faire sur d'autres canaux que le rapport annuel, tels que des magazines spécialisés, site Internet ou autres, celui-ci constitue le document le plus structuré. En tant que document officiel de communication, il constitue le support privilégié pour informer en toute transparence les acteurs concernés. C'est la raison pour laquelle les grands groupes formalisent de plus en plus d'informations relatives à la cybersécurité dans leurs rapports annuels. Le rapport annuel constitue donc une opportunité pour décrire la façon dont l'entreprise se protège et donc indirectement protège les intérêts de ses parties prenantes.

Les données ont donc été étudiées à partir des rapports annuels téléchargés depuis les sites internet institutionnels des entreprises du CAC 40. La liste des sociétés qui composent notre échantillon correspond à celle en date du 31/12/2018. Dans le cas où les entreprises proposent différents documents complémentaires, nous avons exclu les rapports annuels synthétiques et consulté la version complète du document de référence qui intègre le rapport annuel ainsi que le rapport social ou environnemental (les appellations pouvant changer d'une entreprise à l'autre).

Notre démarche méthodologique est mixte : dans un premier temps, nous avons conduit une étude qualitative par analyse de contenu thématique, puis celle-ci a été complétée par une analyse statistique des données récoltées. En ce qui concerne l'étude qualitative, nous avons effectué une lecture approfondie des sections sur les risques opérationnels et plus spécifiquement ceux consacrés aux risques cyber afin d'identifier et d'extraire les différentes thématiques abordées dans les rapports. Cette lecture a été réalisée à partir de la grille d'analyse issue de la littérature (cf. Tableau 1). En particulier, nous avons pu nous appuyer sur les différentes rubriques identifiées dans la littérature (qualification/ gouvernance/ process/ atténuation du risque). Cette grille d'analyse a été adaptée et modifiée en fonction des contenus identifiés dans les rapports annuels. Nous avons effectué un double codage manuel : chaque auteur a lu et codé les 40 rapports annuels. Le codage a consisté à classer les différents extraits du rapport annuel au sein des thématiques préalablement identifiées à l'aide de la grille de lecture issue de la littérature. Les grilles obtenues par auteur ont fait l'objet d'une comparaison pour s'assurer de la fiabilité du codage. Quand les codages étaient discordants, nous avons consulté à nouveau les quelques rapports annuels concernés pour identifier les causes de divergence et s'accorder sur le codage à retenir. Au total, cinq rapports ont été concernés par cette relecture. Nous avons pu ainsi constituer des fiches d'identité relative à la gestion des risques cyber en faisant ressortir pour chacune des entreprises les risques cyber identifiés, les conséquences des risques, leur mode de gouvernance et enfin, les actions de prévention, moyens de détection et de contrôle de ces risques.

Dans un second temps, nous avons préparé les données en vue d'un traitement quantitatif. Nous souhaitions en effet établir un positionnement multidimensionnel dont l'objectif est de représenter chaque objet par un point dans un espace euclidien de dimension aussi faible que possible, de façon à ce que deux objets semblables soient représentés par deux points proches l'un de l'autre, et un couple dissemblable par des points éloignés.

Cette méthode se déroule en plusieurs étapes. La première a consisté à établir un tableau disjonctif à partir de la grille d'analyse que nous avions élaborée. Nous avons substitué les extraits de phrase par un codage disjonctif. Lorsque le thème était présent nous codions 1 lorsqu'il était absent 0. Notons que ce tableau disjonctif nous a permis également de calculer des scores pour chaque dimension de la grille d'analyse. Afin de pouvoir comparer les entreprises, ces scores ont été standardisés.

Dans une seconde étape, nous avons transformé les données initiales en matrice de similitude. La

procédure “proximities” de SPSS permet de calculer les proximités ou les écarts entre les individus sur la base d’indices de similarité/dissimilarité. Le prototype de ces indices est le coefficient de corrélation linéaire. L’ensemble de ces dissimilarités entre paires d’objets est regroupé dans une matrice dite « matrice de dissimilarité ». La diagonale de cette matrice est composée de zéro puisqu’un objet n’est pas différent de lui-même. Les termes hors-diagonaux, quant à eux, représentent les distances Euclidiennes entre paires d’objets.

Dans une dernière étape, nous avons utilisé la procédure ALSCAL de SPSS qui permet de construire des structures géométriques multidimensionnelles, le plus souvent bi ou tridimensionnelles, s’ajustant au mieux aux similarités ou dissimilarités observées ou calculées. L’algorithme de positionnement multidimensionnel utilisé par ALSCAL est directement issu des travaux de Forrest W. Young, (Young, Takane et Lewyckyj, 1978). Il s’agit alors de minimiser une fonction appelée « SSTRESS » (Squared STRESS). Le STRESS étant un indicateur variant entre 0 et 1, la valeur nulle indique un ajustement parfait.

La qualité de l’ajustement peut aussi être jugée grâce à l’indicateur R2, coefficient de corrélation au carré. Dans notre cas, le SSTRESS est de 0,23 et le R2 de 0,69.

4. RESULTATS ET DISCUSSION

La cartographie des entreprises du CAC 40 en matière de cyber-résilience réalisée avec la procédure ALSCAL de SPSS présente deux axes (cf. figure 1).

Le premier axe (« Dimension 1 ») de la représentation est toujours celui correspondant aux écarts observés les plus importants en termes de disparités. Dans la cartographie représentée, la dimension 1 représente le niveau de communication d’informations relatives aux risques cyber. Les entreprises situées les plus à gauche correspondent aux entreprises qui communiquent le plus. A l’inverse, les entreprises situées le plus à droite correspondent à celles qui communiquent le moins. Cette distinction permet de souligner comment les entreprises perçoivent et traitent la transparence en termes de communication sur le management des risques cyber.

Le second axe (« Dimension 2 ») est orienté selon une direction orthogonale au premier, correspondant aux écarts les plus importants parmi ceux qui ne relèvent pas du premier axe. Ici, la dimension 2 est liée au mode de gouvernance spécifique à la cybersécurité.

En bas, il s’agit des entreprises ayant mis en place une gouvernance spécifique et en haut du graphique, celles qui n’ont pas de gouvernance

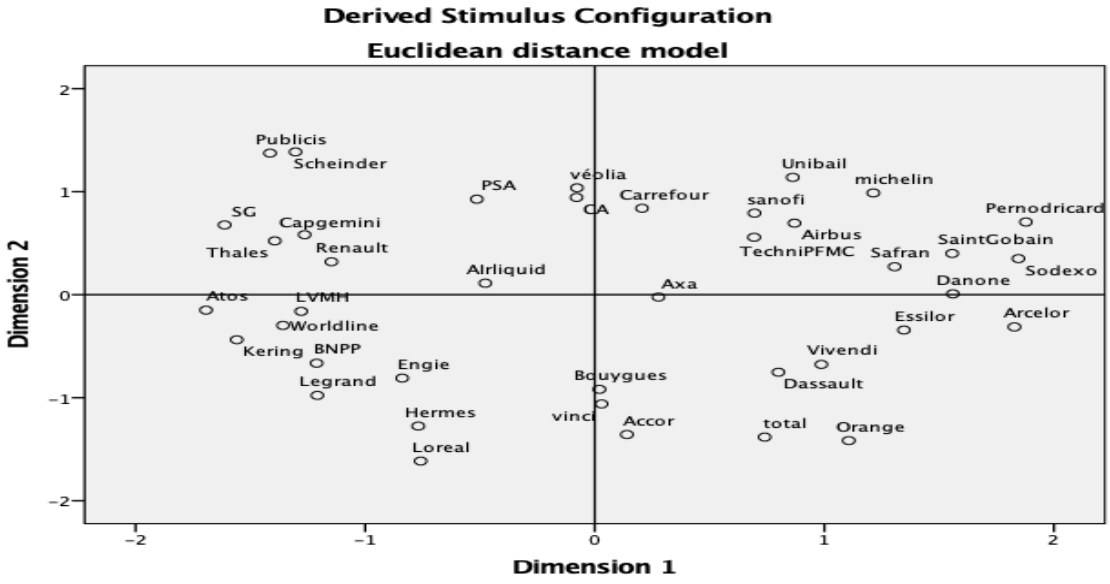

Figure 1 : Cartographie des entreprises

spécifique dédiée. Cette distinction témoigne d'un degré d'engagement variable pour la gestion des risques cyber.

Cette représentation graphique permet une lecture plus simple des données, on peut ainsi y dégager des constatations et découvrir des structures qui seraient passées inaperçues sans représentation. Les entreprises les plus matures dans leur communication relative aux risques cyber sont donc situées dans le rectangle situé en bas à gauche ; les entreprises les plus matures étant notamment Atos, Kering, LVMH ou Wordline. A l'inverse, les entreprises les moins matures sont situées dans le rectangle situé en haut à droite. C'est le cas des entreprises comme Danone, Sodexo, Pernod Ricard ou encore ArcelorMittal. On distingue donc des entreprises plus ou moins proactives dans leur communication sur les risques cyber : certaines entreprises perçoivent et traitent la communication sur les risques cyber de façon transparente, quand d'autres sont en revanche très opaque.

La figure 2 retrace les scores standardisés que nous avons calculés pour chaque dimension de notre grille d'analyse. Dans une lecture sectorielle de cette figure on peut identifier plusieurs éléments saillants. Le secteur du luxe apparaît comme le secteur ayant la plus forte communication sur les risques cyber et le plus mature par la mise en place d'une gouvernance dédiée. Ce résultat peut s'expliquer par l'importance de la protection de leur image de marque et la nécessité de protéger les savoir-faire et secrets de fabrication. En outre, la captation des données personnelles est identifiée comme un risque majeur de l'image de marque de ces entreprises en raison de la qualité de la clientèle, très fortunée et donc particulièrement attractive. Le secteur aéronautique communique très peu à l'exception de Thalès. On pourrait en déduire une méconnaissance du problème cyber. Le monde informatique titre d'ailleurs en 2019 que "le secteur de l'aviation est à la traîne en matière de cybersécurité" alors que les enjeux sont considérables dans ce secteur. Une cyberattaque d'un avion vol induit un risque vital pour les passagers voire autres conséquences catastrophiques. Le cas de Thales est particulier dans la mesure où le groupe propose des solutions en matière de cybersécurité.

Ils se doivent donc d'être exemplaires pour leur client. Concernant le secteur bancaire, celui-ci semble avoir pris la mesure de l'importance d'une politique de cybersécurité. On constate en effet une communication importante de la part des banques. Rien d'étonnant compte tenu de l'exposition majeure de ces dernières aux risques cyber. Les services financiers subissant en moyenne 300 fois

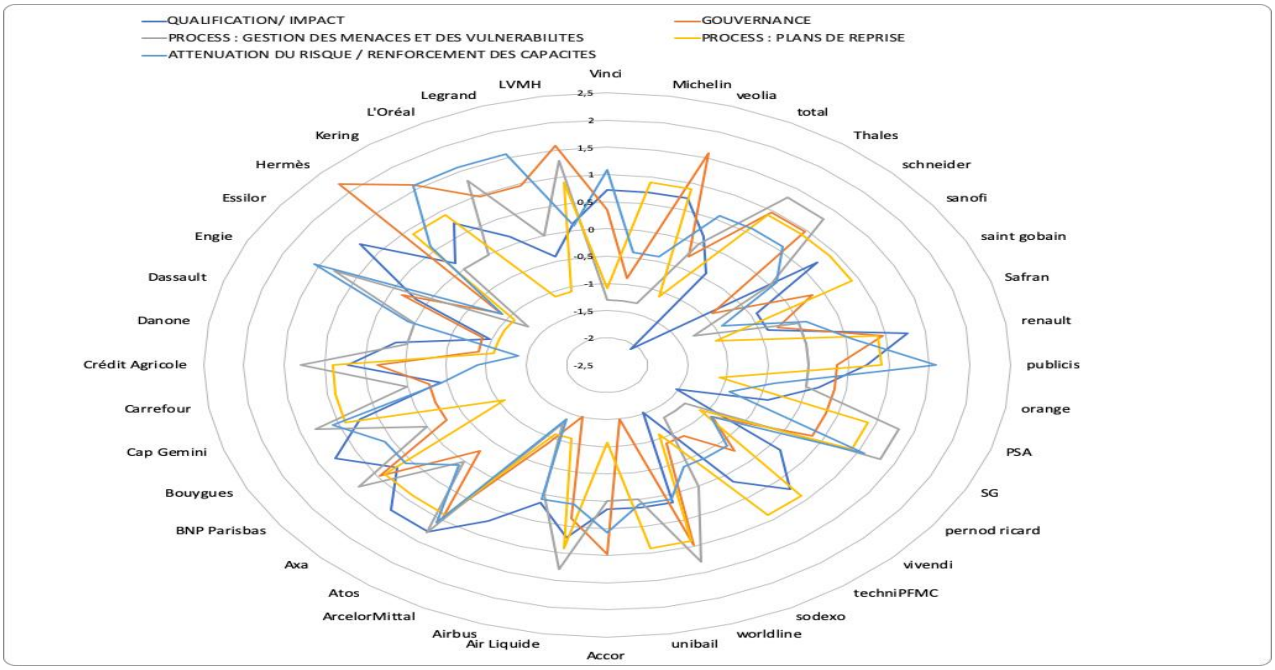

Figure 2 : Positionnement des entreprises sur les différentes dimensions

plus de cyberattaques que les entreprises d'autres secteurs. On notera la maturité de BNP Paribas en la matière avec la mise en place d'une gouvernance spécifique. Le secteur automobile pour sa part communique de façon relativement importante sur la gestion des menaces et des vulnérabilités. Avec le développement de la numérisation notamment l'intégration de composants intelligents et de systèmes intégrés, la cybersécurité devient un enjeu majeur particulièrement avec le développement des véhicules autonomes. La nouvelle norme ISO/SAE 21434 qui permet d'intégrer les questions de cybersécurité à tous les stades du processus de développement oblige les acteurs du secteur à prendre la mesure de ce risque.

Notre étude empirique nous a permis de faire ressortir différents résultats. En premier lieu, notre étude permet d'établir une cartographie des pratiques de communication en matière de risques cyber par les entreprises du CAC 40 en nous appuyant sur une méthodologie réalisée à l'aide de la procédure ALSCAL de SPSS. L'analyse de cette cartographie fait ressortir une forte hétérogénéité, alors que tous ces grands groupes devraient être avancés sur ce sujet majeur vu les conséquences catastrophiques identifiées. La représentation graphique que nous avons pu établir met en évidence une forte disparité de pratiques en matière de communication sur les risques cyber. Si certaines entreprises communiquent très peu sur la cybersécurité, comme Arcelor ou Danone, d'autres sont en revanche très matures sur cette question, voire clairement cyber-résiliente. C'est notamment le cas des groupes Kering, L'Oréal ou Hermès. Pour ces entreprises, plusieurs caractéristiques communes peuvent être soulignées : les risques cyber sont largement cités dans le rapport annuel, ces entreprises mettent en place une gouvernance dédiée à ce risque (équipe spécifique, Délégué à la Protection des Données - DPO), une cartographie des risques en matière d'*Intelligence Artificia*l (IT) est élaborée, des plans de détection spécifiques sont mis en place, des plans d'action sont détaillés en cas d'attaque, ainsi qu'une assurance dédiée aux risques cyber est contractée. Pour certaines entreprises, la protection est parfois étendue jusqu'aux partenaires et sous-traitants, même s'ils sont souvent difficilement maitrisables (Chehbi Gamoura, 2021). Enfin, certaines entreprises mettent en avant la mise en œuvre de la norme ISO 27001 dédiée à la sécurité des systèmes d'information. Au vu de l'hétérogénéité en matière de communication des risques cyber, il est difficile de comparer les entreprises entre elles, tant les pratiques de communication diffèrent d'une entreprise à une autre, alors même que les entreprises appartiennent parfois au même secteur. Ces résultats rejoignent ceux observés par Héroux et Fortin (2020) et PWC (2018) qui mettent en évidence des niveaux de protection et de sensibilisation face aux risques cyber très différenciés entre les entreprises.

Plusieurs arguments peuvent être avancés pour expliquer les différences en matière de communication. Selon l'étude de Cheong et al. (2021), plusieurs raisons peuvent expliquer pourquoi les entreprises ne communiquent pas toujours les informations relatives aux risques cyber. Certaines entreprises peuvent choisir de façon stratégique de diffuser un nombre limité d'informations pour ne pas renseigner ses parties prenantes externes sur d'éventuelles cyberattaques qu'auraient subi l'entreprise et ainsi paraître vulnérable. La diffusion d'informations précises relatives à une cyberattaque pourrait en effet accroître la vulnérabilité de l'entreprise en communiquant des informations sensibles, susceptibles de renseigner de futures attaques (Afterman, 2015). Dans la plupart des cas, les entreprises ont besoin de temps pour détecter une violation de la cybersécurité. Il peut donc exister un déficit dans la détection de l'attaque, par conséquent les risques et incidents ne sont pas détectés rapidement, ni exposés publiquement. Enfin, les dirigeants peuvent également volontairement dissimuler des informations liées à une cyberattaque qui risqueraient de nuire à la réputation de leur entreprise (Cheong et al., 2021). Il est également possible d'envisager une autre explication à une faible diffusion d'information sur les risques cyber, l'entreprise peut estimer ce risque comme relativement faible la concernant, ou alors le risque est bien pris en compte par le groupe, mais celui-ci a mis en place peu de procédures pour se

protéger. Enfin, l'entreprise peut également avoir mis en place en interne un certain nombre d'actions, mais elle a volontairement ou non peu communiqué sur ce qui a été réalisé en matière de protection contre les risques cyber.

Dès lors, se pose la question du niveau optimal en matière de publication relative aux risques cyber. Une publication de trop nombreuses informations peut en effet constituer une surcharge d'information et être mal perçue par les parties prenantes et réduire leur confiance. A l'inverse, une absence ou de très faibles informations communiquées peuvent également susciter de la méfiance ou inquiéter les investisseurs qui pourraient supposer que l'entreprise est mal protégée. On peut donc supposer qu'il existerait un niveau optimal de communication permettant aux différentes parties prenantes d'être rassurées sur les actions mises en place. De même, les investisseurs qui suivent de près l'entreprise pourraient être rassurés et leur confiance renforcée par un niveau de communication suffisant. Une communication efficace pourrait même attirer de nouveaux investisseurs. Il s'agit donc de trouver un équilibre entre sur et sous-divulgation des informations relatives à la cybersécurité (Ferraro, 2014).

Ces divergences en matière de communication viennent également du fait qu'à ce jour, il n'existe pas de standardisation des informations publiées par les entreprises en matière de cybersécurité. Les informations contenues dans les rapports annuels sont encore loin d'être normalisées et il a été difficile de recenser l'ensemble des informations sur les risques cyber pour chacune des entreprises. La plupart des entreprises les identifient en tant que "risques opérationnels", ou les précisent dans une rubrique dédiée aux systèmes d'information. Pour d'autres, les informations relatives à ces risques sont disséminées dans le document. Si pour la RSE, les informations répondent à des critères spécifiques de communication permettant d'harmoniser et de comparer les informations d'une entreprise à l'autre, pour la cybersécurité, c'est loin d'être le cas. Différents auteurs, notamment Takahashi et al. (2010) suggèrent d'ailleurs de standardiser l'information en matière de cybersécurité. La Plateforme RSE[3] qui regroupe des administrations, organisations représentant les entreprises, les organisations syndicales et des représentants de la société civile a pour objectif d'émettre des avis et des recommandations sur les questions sociales et environnementales soulevées par la RSE. A ce titre, la plateforme RSE aborde la notion de Responsabilité Numérique des Entreprises (RNE) dont la définition est la suivante : "La RNE est un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de confiance, de redevabilité, d'éthique et d'échanges avec les parties prenantes des entreprises."

Le 21 juin 2022, un accord relatif aux informations extra-financières, appelé CSRD pour *Corporate Sustainability Reporting Directive,* a été trouvé par le Parlement européen, le Conseil européen et la Commission européenne. Cet accord vise à remplacer la directive 2014/95/UE sur les informations non financières ("Non Financial Reporting Directive" - NFRD). En effet, jusqu'à présent, la transposition de cette directive était très variable selon les États membres avec des exigences de reporting très variables. Cette nouvelle directive vise à imposer aux entreprises européennes de publier annuellement un reporting extra-financier exhaustif et précis. L'application de cette directive se fera dans un premier temps dès le 1er janvier 2024 pour les entreprises déjà soumises à la directive sur les rapports financiers. Elle devrait également par la suite être étendue aux autres grandes entreprises, puis aux PME. La mise en place de cette directive devrait ainsi favoriser une plus grande harmonisation entre les données publiées, facilitant les comparaisons entre entreprises et tout en offrant aux entreprises en situation de retard dans le domaine de la cybersécurité la possibilité d'anticiper un programme d'interventions visant à renforcer leur sécurité. Cette harmonisation est

[3]https://www.strategie.gouv.fr/reseau-france-strategie/plateforme-rse

d'autant plus nécessaire que les agences de notation intègrent déjà les risques cyber dans leur notation financière. Les notations ESG (Environnement Société, Gouvernance), de plus en plus répandues, prennent également déjà en compte les risques cyber.

5. CONCLUSION

Les conséquences d'une cyberattaque sont catastrophiques pour une entreprise en termes de pertes de données, pertes financières ou perte de confiance ou encore d'atteinte à la réputation. Les entreprises doivent donc mettre en place des mesures pour se protéger contre d'éventuelles attaques. Notre recherche exploratoire avait pour objectif d'identifier les informations communiquées par les entreprises sur les actions mises en œuvre pour se protéger d'éventuelles cyberattaques. Nous sommes partis de l'hypothèse qu'une entreprise particulièrement active en matière de cybersécurité voire de cyber-résilience aura intérêt à en faire la communication dans son rapport annuel pour en informer ses différentes parties prenantes dans l'objectif de les rassurer et de montrer son degré de maturité et de résilience. L'intérêt d'une telle étude est de proposer un modèle d'évaluation de la maturité cyber des organisations, à travers l'élaboration d'une cartographie. Notre revue de la littérature nous a permis de définir les facteurs à prendre en compte pour évaluer la cyber-résilience d'une entreprise. Il s'agit notamment de la sensibilisation et de la formation de l'ensemble des collaborateurs, la mise en place de plans d'actions et de continuité d'exploitation après une attaque, la souscription d'une assurance dédiée ou encore d'une gouvernance spécifique.

Les résultats de notre étude apportent plusieurs contributions, notamment à la littérature sur les informations extra-financières et sur celle liée aux risques cyber. Premièrement, l'étude contribue à la littérature sur la divulgation des entreprises sur les risques cyber afin d'évaluer la cyber-résilience des organisations. Elle a permis d'aboutir à l'établissement d'une cartographie des entreprises du CAC 40 qui permet de visualiser leur degré de maturité cyber en regard de leur communication. Les recherches réalisées dans le domaine de la comptabilité et des systèmes d'information se concentrent principalement sur les réactions du marché à la suite d'incidents de cybersécurité et ont examiné un ensemble de facteurs de contingence tels que le type de brèches (Gordon et al., 2011 ; Yayla et Hu, 2011), les caractéristiques des entreprises (Ettredge et Richardson, 2003) et les informations divulguées par le biais d'articles de presse (Wang et Park, 2017) et de canaux de distribution (Benaroch et al., 2012) qui pourraient approfondir ou atténuer la réaction du marché, tandis que seules quelques études prennent en compte la divulgation relative aux risques cyber. Nos résultats mettent en évidence une grande hétérogénéité dans le niveau de maturité des entreprises du CAC 40, alors qu'on aurait pu s'attendre à ce que les grandes firmes multinationales soient toutes assez matures. Les risques cyber étant largement connus et considérés comme majeurs, il paraît alors surprenant que certaines grandes entreprises ne le mentionnent presque pas dans leur rapport annuel. Pour mieux comprendre les motivations des entreprises sur leur degré de communication, il serait intéressant de compléter cette étude sur les rapports annuels des sociétés du CAC 40 par des entretiens semi-directifs auprès des décideurs. Notre étude suggère différentes pistes pour orienter les décisions et actions des dirigeants et responsables de la sécurité des entreprises. En particulier, en identifiant leur niveau de communication des informations relatives à la cybersécurité, les entreprises peuvent ainsi décider si leur communication doit être renforcée ou au contraire atténuée. Dans l'ensemble, nos résultats suggèrent une meilleure prise de conscience des risques cyber ainsi qu'une sensibilisation accrue des collaborateurs. Enfin, nos résultats font également ressortir que certaines entreprises ayant une faible communication et une faible gouvernance en matière de cybersécurité devraient notamment élaborer des plans d'action spécifiques et autres plans de détection pour renforcer leur posture en matière de cybersécurité. Notre cartographie des entreprises permet donc aux entreprises de mieux évaluer leur maturité cyber pour décider des actions spécifiques à mettre en place, ajuster leur communication et se conformer aux réglementations sur la cybersécurité

qui ne cessent d'évoluer. Enfin la mise en place de standards de reporting harmonisés semble nécessaire pour assurer une meilleure transparence et harmonisation et permettre une comparaison entre les entreprises. Une telle standardisation permettrait d'établir des relations plus fiables et transparentes avec les différentes parties prenantes.

Les limites de cette étude sont liées au fait que l'analyse des rapports annuels ne permet pas de rendre directement compte des actions menées au sein de l'entreprise, mais des actions qu'elle communique volontairement. La grande disparité observée dans les résultats de notre étude vient notamment d'une absence de référentiel commun et d'obligations légales de reporting extra-financier en matière de risques cyber. Une harmonisation et standardisation des pratiques de reporting extra-financier et de définition d'indicateurs de performance permettrait davantage de transparence et de comparabilité entre les entreprises, tout en prenant la mesure de ce qui compte pour les parties prenantes, à l'instar du développement des indicateurs de l'Economie circulaire (Bonet Fernandez et al. 2014). Il serait enfin pertinent d'étudier l'impact de la communication sur les risques cyber sur la perception des parties prenantes.

6. BIBLIOGRAPHIE

Altintas, G. (2020). La capacité dynamique de résilience : l'aptitude à faire face aux événements perturbateurs du macro-environnement. *Revue management et avenir*, (1), 113-133. https://doi.org/10.3917/mav.115.0113

Altintas, G., & Royer, I. (2009). Renforcement de la résilience par un apprentissage post-crise : une étude longitudinale sur deux périodes de turbulence. *M@n@gement*, *12*(4), 266-293. https://doi.org/10.3917/mana.124.0266

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177-1206.

Anderson, R., Barton, C., Bohme, R., Clayton, R., Eeten, M. J. G., Levi, M., & Savage, S. (2012). Measuring the Cost of Cybercrime, WEIS. https://doi.org/10.1007/978-3-642-39498-0_12

Arpagian N., (2018), La cybersécurité, *Presses Universitaires de France*, « Que sais-je ? ».

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22 (3), 251-264. https://doi.org/10.1108/IMCS-02-2013-0014

Bahl, L., Gagné, V. et Corriveau, A. (2021). Cybersécurité, légitimité et étendue de la divulgation aux rapport annuels d'entreprises canadiennes. La fuite de données personnelles chez Desjardins. *41ème congrès de l'AFC*, mai.

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal: A Global Perspective*. 28(6), 164-177. https://doi.org/10.1080/19393555.2019.1689318

Bakker, T. G., and K. Streff. 2016. Accuracy of self disclosed cybersecurity risks of large U.S. banks. *Journal of Applied Business and Economics*. 18 (3), 39–51. https://articlegateway.com/index.php/JABE/article/view/848

Ben Jabeur, S., & Serret, V. (2019). Principes et enjeux de la responsabilité des conseils d'administration face au risque cybernétique. *Question (s) de management*, (4), 67-76. https://doi.org/10.3917/qdm.194.0067

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy,* 37 (6), 508-526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on *Risk and Insurance-Issues and Practice*, 40, 131-158. https://doi.org/10.1057/gpp.2014.19

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience - Fundamentals for a Definition. WorldCIST. https://doi.org/10.1007/978-3-319-16486-1_31

Bonet Fernandez, D., Petit, I., & Lancini, A. (2014). L'économie circulaire : quelles mesures de la performance économique, environnementale et sociale ? *Revue Française De Gestion Industrielle*, 33(4), 23–43. https://doi.org/10.53102/2014.33.04.791

Caralli, R. A. (2006). Sustaining Operational Resiliency: A Process Improvement Approach to Security Management. Carnegie-Mellon Univ. Pittsburgh pa software engineering inst. https://doi.org/10.1184/R1/6584495.v1

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010), August. Improving operational resilience processes: The CERT resilience management

model. In *IEEE Second International Conference on Social Computing* (pp. 1165-1170).
https://doi.org/10.1109/SocialCom.2010.173

Chebi Gamoura, S. (2021). Processus Achat 5.0 et Acheteurs Augmentés : L'IA collective avec chat-bots dotés d'aversion au risque post-COVID-19: Cas d'un constructeur automobile Français. *Revue Française De Gestion Industrielle*, 36(1), 83–111.
https://doi.org/10.53102/2022.36.01.907

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of information Systems*, *35*(2), 179-194.
https://doi.org/10.2308/ISYS-2020-031

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4 (10,). 13-21.
https://doi.org/10.22215/timreview/835

Curtis, P. D., & Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In *2015 IEEE international symposium on technologies for homeland security (hst),* April*,* 1-6.
https://doi.org/10.1109/THS.2015.7225323

DeCoste, J. (2017). The impact of cyber-attacks on publicly traded companies (Doctoral dissertation, Concordia University).

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43-57.
https://doi.org/10.1353/jod.2010.0010

Deloitte, (2016), Cyberattaques : comment chiffrer les impacts ? Le visible et l'invisible. [En ligne] (consulté le 12 avril 2022) Disponible à l'adresse : https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/cyberattaques-chiffrer-les-impacts.html

Derrouiche, R. (2022). Supply Chain 4.0 : rôles et opportunités de la gestion industrielle. *Revue Française de Gestion Industrielle*, 36(1), 124–129.
https://doi.org/10.53102/2022.36.01.1111

Douzet, F. et Héon, S. (2013). L'analyse du risque cyber, emblématique d'un dialogue nécessaire. *Sécurité et stratégie*, 14 (3),44-52.
https://doi.org/10.3917/sestr.014.0044

Dupont, B., Shearing, C. Bernier, M., Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice, *Computers & Security*, 132.
https://doi.org/10.1016/j.cose.2023.103372

Eddé, R. (2020). Les entreprises à l'épreuve des cyberattaques. *Flux*, 121, 3, 90-101.
https://doi.org/10.3917/flux1.121.0090

Eijkelenboom, E.V.A. & Nieuwesteeg, B.F.H.. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*, 40.
https://doi.org/10.1016/j.clsr.2020.105513

Eling, M. & Wirfs, J., (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, Elsevier, 272 (3), 1109-1119.
https://doi.org/10.1016/j.ejor.2018.07.021

Erkens, M., Paugam, L. & Stolowy, H. (2015). Non-financial information: State of the art and research perspectives based on a bibliometric study. *Comptabilité Contrôle Audit*, 21(3), 15-92.
https://doi.org/10.3917/cca.213.0015

Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & security*, *97*.
https://doi.org/10.1016/j.cose.2020.101996

Gao L., Calderon T.G. & Tang F. (2020), Public companies' cybersecurity risk disclosures, *International Journal of Accounting Information Systems,* 38.
https://doi.org/10.1016/j.accinf.2020.100468

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People* 22 (2), 92-108.
https://doi.org/10.1108/09593840910962186

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, 19(1), 33-56. https://doi.org/10.3233/JCS-2009-0398

Grøtan, T. O., Antonsen, S., & Haavik, T. K. (2022). Cyber resilience: a pre-understanding for an abductive research agenda. In *Resilience in a Digital Age: Global Challenges in Organisations and Society*, 205-229. Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-85954-1_12

Hamel, G. & Valinkangas, L. (2003). The Quest for Resilience. *Harvard Business Review.* 81(9), 52-65.

Häring, I., Ebenhöch, S., Stolz, A., (2016). Quantifying resilience for resilience engineering of socio-technical systems. Eur. J. *Secur*. Res. 1 (1), 21–58.
https://doi.org/10.1007/s41125-015-0001-x

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, *34*(2), 187-209. https://doi.org/10.2308/isys-18-053

Héroux S. & Fortin A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, 19 (2), 73-100.
https://doi.org/10.1111/1911-3838.12220

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: who cares?. *Georgetown McDonough School of Business Research Paper*. https://dx.doi.org/10.2139/ssrn.2852519

Jenkins, H., & Yakovleva, N. (2006). Corporate social responsibility in the mining industry: Exploring trends in social and environmental disclosure. *Journal of cleaner production*, *14*(3-4), 271-284. https://doi.org/10.1016/j.jclepro.2004.10.004

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749. https://dx.doi.org/10.2139/ssrn.3135514

Kemmerer, R. A. (2003). Cybersecurity. In *25th International Conference on Software Engineering, May. Proceedings.* 705-715. IEEE. https://doi.org/10.1109/ICSE.2003.1201257

Keys, B., & Shapiro, S. (2019). Frameworks and best practices. *Cyber Resilience of Systems and Networks*, 69-92. https://doi.org/10.1007/978-3-319-77492-3_4

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25* (1), 1-10. https://doi.org/10.3233/THC-161263

Le, N. T., & Hoang, D. B. (2016). Can maturity models support cybersecurity? In *IEEE 35th international performance computing and communications conference (IPCCC),* December, 1-7. https://doi.org/10.1109/PCCC.2016.7820663

Lehu, J. M. (2018). Cyberattaque : la gestion du risque est-elle encore possible? Analyse et enseignements du cas Sony Pictures. *La revue des sciences de gestion*, (3-4), 41-50. https://doi.org/10.3917/aprp.003.0026

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies, 9.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171. https://doi.org/10.2308/ajpt-52593

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40-55. https://doi.org/10.1016/j.accinf.2018.06.003

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25. https://doi.org/10.1007/978-3-319-77492-3_1

Mereuil A. de & Bonnefous A.-M. (2016), Anatomie d'une cyber-attaque contre une entreprise : comprendre et prévenir les attaques par déni de service, *Annales des Mines-Gérer et comprendre*, 5-14. https://doi.org/10.3917/geco1.123.0005

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, *26* (3), 565-584. https://doi.org/10.1287/isre.2015.0587

Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defence for the business entity: A prerequisite corporate policy. Academy of Strategic Management Journal, 15 (2), 15.

Nurse, J. R. C., Creese, S., Goldsmith, M. & Lamberts, K. (2011) Trustworthy and Effective Communication of Cybersecurity Risks: A Review. In: The 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), *The 5th International Conference on Network and System Security* (NSS). https://doi.org/10.1109/STAST.2011.6059257

Orchiston, C., Prayag, G., & Brown, C. (2016). Organizational resilience in the tourism sector. *Annals of Tourism Research*, *56*, 145-148. https://doi.org/10.1016/j.annals.2015.11.002

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172-196. https://doi.org/10.1287/deca.2018.0387

Pardini, D. J., Heinisch, A. M. C. & Parreiras, F. S. (2017). Cyber Security Governance and Management for Smart Grids in Brazilian Energy Utilities. *Journal of Information Systems and Technology Management*, 14, 385-400. https://doi.org/10.4301/s1807-17752017000300006

Proag, V. (2014). The concept of vulnerability and resilience. *Procedia Economics and Finance*, *18*, 369-376. https://doi.org/10.1016/S2212-5671(14)00952-6

Putra, A. P. G., Humani, F., Zakiy, F. W., Shihab, M. R., & Ranti, B. (2020). Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia. In *International Conference on Information Technology Systems and Innovation (ICITSI), October,* IEEE, 89-94 https://doi.org/10.1109/ICITSI50517.2020.9264982

PWC (2020), « Enquête – Les priorités du Directeur Financier, Concilier sens et complexité », en partenariat avec la DFCG.

Rapport France Stratégie, (2020). Responsabilité numérique des entreprises.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Rothrock, R. A., Kaplan, J. & Van der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review,* 59 (2), 12–15. https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Senkel, M-P. (2009). La divulgation d'informations « RSE » par les prestataires de services logistiques européens : Une analyse comparative du site Internet et du rapport d'activité », *Marché et organisations*, 8 (1), 173-200. https://doi.org/10.3917/maorg.008.0173

Sepúlveda Estay D., A., Sahay, R., Barfod, M. B., Jensen, C., D. (2020), A systematic review of cyber-resilience assessment frameworks*, Computers & Security*, 97. https://doi.org/10.1016/j.cose.2020.101996

Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 23(2), 1-11.

Wang P. & Park, S-A. (2017) Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems*, 18 (2), 136-147. https://iacis.org/iis/2017/2_iis_2017_136-147.pdf

Weick, K. E., & Sutcliffe, K. M. (2011). Managing the unexpected: Resilient performance in an age of uncertainty (Vol. 8). John Wiley & Sons.

White, G. B. (2011). The community cyber security maturity model. In *IEEE international conference on technologies for homeland security (HST),* November. 173-178. https://doi.org/10.1109/THS.2011.6107866 .

Whitler, K. A. & Farris, P. W. (2017), The impact of cyber-attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, 2017, 57 (1), 3-9. https://doi.org/10.2501/JAR-2017-005

Yilmaz Borekci, D., Rofcanin, Y., & Gürbüz, H. (2015). Organisational resilience and relational dynamics in triadic networks: a multiple case analysis. *International Journal of Production Research*, *53*(22). https://doi.org/10.1080/00207543.2014.903346

Young, F. W., Takane, Y., & Lewyckyj, R. (1978). ALSCAL: A nonmetric multidimensional scaling program with several individual-differences options. *Behavior Research Methods & Instrumentation*, *10*(3), 451-453. https://doi.org/10.3758/BF03205177

Zhang, X. A., & Borden, J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, *23*(10), 1336-1352. https://doi.org/10.1080/13669877.2019.1646315

7. BIBLIOGRAPHIE

Anne-Laure Farjaudon est Maître de conférences à l'IAE Bordeaux et est membre de l'équipe de recherche de l'IRGO (Institut de Recherche en Gestion des Organisations). Elle est responsable du Mater 1 Contrôle de gestion et Audit Interne, ainsi que de la filière Expertise-comptable. Ses recherches sont ancrées principalement dans le champ du contrôle de gestion, de la comptabilité et de l'audit et portent notamment sur l'immatériel, la RSE et l'information extra-financière comme c'est le cas dans le papier proposé.

Nathalie Gardès est Maître de conférences HDR à l'IUT de Bordeaux et est membre de l'équipe de recherche de l'IRGO (Institut de Recherche en Gestion des Organisations). Elle est responsable de la licence professionnelle Métiers de l'immobilier. Ses recherches portent sur l'impact du numérique sur les organisations à travers différents prismes : expérience client, transformation digitale, appropriation des technologies.

[1] **Anne-Laure Farjaudon,** Univ. Bordeaux, IRGO, EA 4190, F-33000 Bordeaux, France, anne-laure.farjaudon@u-bordeaux.fr ,

[2] Nathalie Gardès, Univ. Bordeaux, IRGO, EA 4190, F-33000 Bordeaux, France, nathalie.gardes@u-bordeaux.fr