DIVULGATION D'INFORMATION SUR LA CYBERSÉCURITÉ

Objet : Divulgation d'informations sur la cybersécurité : les déterminants, les facteurs qui influent sur la décision de divulguer, la réaction des différentes parties prenantes

Théories : la théorie de la légitimité et la théorie des parties prenantes seront mobilisées pour expliquer la divulgation d'informations sur la cybersécurité.

Méthodes : une méthodologie mixte sera utilisée. Elle combinera une partie qualitative (analyse de contenu, questionnaires et/ou interviews sur les facteurs qui influent sur la décision de divulguer et sur la réaction de différentes prenantes), quantitative (relation qui existe entre les différentes variables utilisées dans la divulgation sur les informations sur la cybersécurité) ou mixte (déterminant de cette forme de divulgation)

Contribution : cette étude contribuera à mieux comprendre les motivations de la divulgation des informations sur la cybersécurité et complétera la littérature sur la divulgation en matière de cybersécurité.

Introduction

Aujourd'hui la technologie a pris de l'ampleur dans la vie des entreprises, les invitant à se (ré)adapter. Cette (ré)adaptation vient aussi avec le risque de fraude et de fuite à caractère cybernautique. Il ne s'agit plus de considérer si le problème de fuite se posera mais de quand il arrivera (Karanja et Rosso, 2017). De ce fait, la question de la cybersécurité devient une des préoccupations majeures des dirigeants d'entreprise (Li et al., 2018). Le terme cybersécurité est utilisé dans plusieurs secteurs et domaines et par divers acteurs. Cependant, il n'y a pas une définition qui fait l'unanimité (Craigen *et al.*, 2014; Porteous, 2018; Schatz *et al.*, 2017). La définition varie selon qu'il s'agisse des entreprises, des gouvernements ou des chercheur.e.s (Schatz *et al.*, 2017). Ainsi, pour Schatz *et al.* (2017), « par cybersécurité, on entend la préservation – par des politiques, par la technologie et par l'éducation – de la disponibilité et de l'intégrité de l'information et de son infrastructure sous-jacente, dans le but d'accroître la sécurité des personnes à la fois en ligne et hors ligne » (Schatz *et al.*, 2017, p. 3). Dans le domaine de la gestion ou de la comptabilité, la cybersécurité peut être définie comme un risque lié à un événement électronique

malveillant qui entraine non seulement des perturbations des activités d'une entreprise mais également des pertes financières (Mukhopadhyay *et al.*, 2013; Öğüt *et al.*, 2011).

La notion de risque apparait dans les définitions et relie la cybersécurité aux activités de l'entreprise. Vu que les activités de l'entreprise peuvent nécessiter un regroupement ou le découpage des projets, on reprend à notre compte certains questionnements de Presley et Landry (2016) à savoir : « *What are the characteristics of a project that would invite attention from potential attackers*?; *What motivations would inspire cyber attacks ?*» (Presley et Landry, 2016, p. 4). Et se demander quel sera le rôle du gestionnaire à chaque étape du projet pour tenir compte des risques à caractère cybernétique. Par exemple, des études sont menées dans l'industrie de la construction pour la création des villes intelligentes (Alshammari *et al.*, 2021; Presley et Landry, 2016; Raimundo et Rosário, 2022), et la prise en compte est à prévoir. Tenir compte des risques est nécessaire mais en informer les différents partenaires de l'entreprise est important pour la prise de décision (Bakker et Streff, 2016); d'où la mise en place des cadres d'évaluation (Dioubate et Daud, 2022; Mukhopadhyay *et al.*, 2013) et de gestion de risques (Dioubate et Daud, 2022; Gordon et Loeb, 2002); et la nécessité de la divulgations d'informations sur la cybersécurité.

Les entreprises devraient-elles divulguer plus d'informations sur la cybersécurité ? Quels facteurs influent sur la décision de divulgation ? Ou encore à quel moment effectuer ces divulgations ? Autant de questions auxquelles des réponses méritent d'être trouvées.

Motivation et pertinence de mener cette recherche

Le stockage, la conservation et la gestion des données sensibles comme la vie privée des différents partenaires (Park et Shin, 2020) font partie intégrante de la vie de l'entreprise. Or le développement et l'accroissement de l'utilisation de la technologie ouvrent la porte à la fraude, à la fuite d'informations et à des cyberattaques. Il devient donc nécessaire que la direction de l'entreprise mette en place des mécanismes pour veiller à la confidentialité, l'intégrité et la disponibilités des données et des informations de l'entreprise (Gordon et Loeb, 2002; Mukhopadhyay *et al.*, 2013) d'une part et d'autre part, communiquer sur les risques de fuite, de fraude et d'attaque (Kamiya *et al.*, 2021). Les coûts associés aux cyberattaques et aux violations des données n'affectent pas seulement l'entreprise mais la société dans son ensemble (D'arcy et Basoglu, 2022, p. 795).

Bien qu'il existe de la littérature sur la cybersécurité dans le domaine de IT, de l'ingénierie et d'autres domaines, en comptabilité par contre, elle est à ses débuts (Kamiya *et al.*, 2021; Karanja et Rosso, 2017; Li *et al.*, 2018; Radu et Smaili, 2021; Smaili *et al.*, 2022).

Plusieurs raisons me poussent à m'intéresser à la divulgation d'informations sur la cybersécurité dans le domaine de la comptabilité et son impact sur la vie d'un projet. D'abord, la cybersécurité est un sujet d'actualité; elle touche presque toutes les structures de l'entreprise. Elle touche à la gestion des risques en général et les différents aspects très particuliers de la protection des données; elle influence la gouvernance (Radu et Smaili, 2021; Smaili *et al.*, 2022), l'éthique et impacte les différents partenaires, tant internes qu'externes de l'entreprise. Ensuite, c'est une problématique nouvelle et son étude permettra de comprendre en profondeur le sujet, surtout avec l'accroissement et l'utilisation des réseaux sociaux par l'entreprise et ses employés. De plus, l'avènement de la Covid 19 a reconfiguré l'espace et l'organisation de travail dans les entreprises (télétravail, téléconférence, ventes en ligne etc.). Enfin, comme c'est un domaine nouveau encore peu exploré, la recherche est à ses débuts, il y a donc une bonne opportunité pour la recherche sur le sujet et ses ramifications sur les projets.

Au regard de ce qui précède, des entrevues avec les Dircteurs des Nouvelles Technologies (Chief Technical Officer - CTO), les gestionnaires et/ou dirigeants pourraient encore préciser les décisions de divulguer de l'information sur la cybersécurité.

Pour ce faire, je prévois contacter les CTO de certaines entreprises. Je vise les entreprises de TX60. Ce sont de grandes entreprises et il y a plus de chance d'y trouver la fonction de CTO. Je m'attends à un taux de retour de 50% (la moitié des entreprises listées sur le TX60). Le but sera de voir comment les CTO regardent les risques de cybersécurité et ce qu'ils décident de divulguer et plus précisément :

1- Leur approche pour identifier les risques,
2- Comment ils gèrent les risques,
3- Leur tolérance aux risques,
4- Leur divulgation en matière de cybersécurité (à quel point ils divulguent leur stratégie, leur crainte par rapport à l'information qui est confidentielle pour ne pas nourrir les fraudeurs etc.).

5- Comment répondent-ils aux demandes des parties prenantes en matière de cybersécurité (comment déterminent-ils et priorisent les parties prenantes importantes – existe-il une cartographie des parties prenantes? Une matrice des plus importantes? Les actions les plus urgentes etc.).
6- Dans une perspective de long terme, prévoient-ils une collaboration avec d'autres entreprises ou partenaires pour une mutualisation des efforts visant la protection des données (qui, pourquoi et comment)?

L'analyse de l'ensemble de ces données une fois collectées, permettra comprendre davantage les raisons profondes de la divulgation d'information sur la cybersécurité.

BIBLIOGRAPHIE

Bakker, T. G. et Streff, K. (2016). Accuracy of Self Disclosed Cybersecurity Risks of Large US Banks. *Journal of Applied Business and Economics*, *18*(3), 39-51.

Craigen, D., Diakun-Thibault, N. et Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10).

Alshammari, K., Beach, T. et Rezgui, Y. (2021). Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction*, *26*, 159-173.

D'arcy, J. et Basoglu, K. A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, *23*(3), 779-805. doi: 10.17705/1jais.00740

Dioubate, B. M. et Daud, W. (2022). A Review of cybersecurity risk management framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(5), 1031-1093.

Gordon, L. A. et Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. et 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.

Karanja, E. et Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23-47.

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

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. et Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11-26.

Öğüt, H., Raghunathan, S. et Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis: An International Journal*, *31*(3), 497-512.

Park, Y. J. et Shin, D. D. (2020). Contextualizing privacy on health-related use of information technology. *Computers in Human Behavior*, *105*, 106204.

Porteous, H. (2018). *Cybersécurité: défis techniques et stratégiques* Bibliothèque du Parlement.

Presley, S. S. et Landry, J. P. (2016). A process framework for managing cybersecurity risks in projects.

Radu, C. et Smaili, N. (2021, 2022/05/01). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. *Journal of Business Ethics*, *177*(2), 351-374. doi: 10.1007/s10551-020-04717-9

Raimundo, R. J. et Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*, *12*(3), 1598.

Schatz, D., Bashroush, R. et Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Smaili, N., Radu, C. et Khalili, A. (2022, 2022/06/22). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*. doi: 10.1007/s10997-022-09637-6