Les dirigeants face aux risques informationnels : étude exploratoire dans le domaine du réseau télécom

Dijana Lekic-Savatic, Anna Lezon Rivière, Madjid Ihadjadene

Les dirigeants face aux risques informationnels : étude exploratoire dans le domaine du réseau télécom

1er axe thématique

DIJANA LEKIC, ANNA LEZON RIVIERE, MADJID IHADJADENE

Mots clés : sécurité de l'information ; risque informationnel ; comportements sécuritaires ; dirigeant ; sense-making methodology

INTRODUCTION

Dans un environnement technologique évolutif, la maîtrise des risques informationnels par les organisations est devenue une problématique complexe qui fait l'objet de nombreuses études [1]. Le risque informationnel se rapporte aux menaces pouvant toucher les actifs matériels et immatériels des organisations [2, 3]. Il est défini comme « la possibilité de dommages, de conséquences négatives ou de résultats indésirables, associés à la sélection, la mise en forme, le transfert et l'utilisation de l'information » [4]. Pour construire une démarche de gestion de ces risques, les organisations définissent et mettent en œuvre un ensemble d'activités et de mesures de sécurité [1, 2, 5]. La réussite de cette démarche dépend, entre autres, des acteurs de l'organisation et de leur conformité avec les mesures adoptées [6, 7]. De ce fait, des scientifiques des domaines divers se sont attachés à étudier les comportements sécuritaires des acteurs et les facteurs les influençant. Cependant, il existe peu de travaux sur la perception des risques informationnels par les cadres dirigeants [8].

Notre communication vise à répondre aux questions suivantes : quels sont les risques informationnels perçus par ces dirigeants ? Quel rôle occupent-ils dans la démarche globale de gestion des risques informationnels ? Quelles mesures sont mises en œuvre pour sécuriser les informations et faire adhérer les équipes à la démarche sécuritaire ? Pour répondre à ces questions, nous nous fondons sur les résultats issus d'une étude empirique qualitative menée avec vingt-deux dirigeants des unités de réseau télécom, dans le contexte d'un grand groupe français.

RISQUES INFORMATIONNELS ET DIRIGEANTS

Dans la littérature, la question des risques informationnels est étudiée selon les trois aspects : technique, organisationnel et humain. Le premier comprend des solutions techniques à mettre en œuvre pour sécuriser les dispositifs informationnels. Le second consiste à définir des politiques de sécurité au niveau de l'organisation. Enfin, le troisième se réfère aux comportements et actions des acteurs internes, aussi bien qu'externes à l'organisation. Certains auteurs postulent que les failles de sécurité sont dues aux comportements des employés [9]. Dans cette communication, nous nous intéressons à la perception des risques informationnels par les cadres dirigeants.

La littérature et les experts de la sécurité de l'information présentent l'implication des dirigeants comme un élément déterminant pour l'efficacité de la démarche de gestion des risques informationnels [10-12]. Williams [13] affirme que leur rôle est de s'assurer de la bonne compréhension et du respect de la politique de sécurité de l'information. Hormis les dirigeants des entreprises, les dirigeants des entités ou des domaines métier jouent un rôle central. Leurs connaissances du domaine permettent d'identifier des informations sensibles et

confidentielles, de maîtriser des coûts liés à la sécurité, en évitant les excès, et d'attribuer des accès à l'information de manière adéquate. Hu et al. [14] ont montré que la participation des dirigeants supérieurs dans les actions de sécurisation de l'information a un impact direct sur la conformité des employés avec les politiques de sécurité. Berthevas [6] a souligné l'importance de leur implication dans l'élaboration de la politique de sécurité de l'information, mais aussi dans sa promotion par des moyens divers de sensibilisation. Straub et Welke [15] ont montré une méconnaissance de certaines mesures et actions de réduction des risques informationnels chez les dirigeants de deux entreprises américaines de traitement et de commercialisation des données. Le même constat a été fait dans une étude plus récente portant sur les aspects de sécurité de l'information dans le contexte de l'espace de travail digital. Les auteurs ont pu constater un manque de connaissances des nouveaux risques informationnels chez les managers hongrois [16]. Enfin, une revue de la littérature réalisée par Soomro et al. [17] a montré que les nombreuses activités managériales contribuent à la qualité de management de la sécurité de l'information.

Des nombreux travaux scientifiques mettent en exergue le rôle du dirigeant dans la gestion des risques informationnels et son influence sur les comportements des employés. Cependant, les comportements des dirigeants et leur perception de la sécurité de l'information sont moins étudiés. S'intéresser à ces acteurs clés permettrait aux organisations d'identifier des faiblesses de la démarche de gestion des risques informationnels, de promouvoir une culture de sécurité et d'inculquer des réflexes comportementaux face aux risques. Notre travail contribue à enrichir ces connaissances apportant des éclairages sur la perception des risques informationnels, ainsi que sur les comportements sécuritaires des dirigeants de réseau télécom.

METHODOLOGIE DE L'ETUDE ET GROUPE D'ACTEURS

Notre étude empirique a été menée dans le cadre d'un projet de recherche au sein d'une grande entreprise française de télécommunications. L'étude s'est concentrée sur les dirigeants des entités du domaine de réseau télécom. Ancrée dans le constructivisme, la méthodologie de recherche consistait en une démarche circulaire et itérative de collecte et d'analyse des données [18]. Pour recueillir les données, nous avons fait appel à des ressources multiples. Tout d'abord, la documentation métier a été collectée dans les dispositifs internes de l'organisation (intranets, espaces collaboratifs, réseau social d'entreprise). L'analyse de cette documentation nous a permis d'acquérir des connaissances sur ce domaine et de préparer l'enquête. Ensuite, nous avons conduit des entretiens téléphoniques selon la méthodologie de construction de sens de Dervin [19]. Les vingt-deux entretiens d'une durée moyenne de 30 minutes ont été enregistrés et transcrits pour le besoin d'analyse.

L'échantillon d'étude était constitué des dirigeants des Unités d'Intervention (UI) et Unités de Pilotage Réseau (UPR)[1]. Les dirigeants disposaient de plusieurs années d'expérience dans le domaine de réseau et exerçaient leurs fonctions à un haut niveau de responsabilité. Leur mission consistait, entre autres, à déployer la stratégie de l'entreprise au sein de l'entité, à organiser et conduire les activités de construction et de maintien des infrastructures de réseau télécom. L'entretien commençait par une courte présentation de l'entité et des fonctions du dirigeant. Il se poursuivait par la demande adressée au dirigeant de se rappeler une situation de travail récente où il avait été confronté à un manque d'information. L'ensemble des données collectées a été analysé selon les méthodologies de construction de sens et de la

[1] Ces entités rassemblent l'ensemble des métiers travaillant dans la construction et la maintenance des réseaux télécom de l'entreprise. Elles disposent des structures opérationnelles et fonctionnelles (ressources humaines, contrôle de gestion, communication) et leur taille va de 300 à plus de 1000 salariés.

théorisation enracinée. Le chercheur examinait le comportement et les actions entreprises par l'acteur selon plusieurs dimensions : cognitive (réflexion, pensées, moments de construction de sens), affective (émotions), situationnelle (besoin informationnel, manque, stratégies de recherche, résultats et usage de l'information).

RESULTATS DE L'ETUDE

L'analyse des données de recherche nous a permis de saisir les enjeux et les contraintes liés aux risques informationnels et à la sécurité de l'information pour les métiers de réseau télécom et, plus précisément, les dirigeants des unités de réseau. Ci-dessous, nous présentons les résultats obtenus.

Responsable de la sécurité de l'information

Considérée comme le capital immatériel des organisations, l'information s'est imposée comme une des préoccupations des dirigeants et un sujet d'importance majeure : « L'information est devenue au centre, on va dire de nos attentions. » (Dirigeant UI, EN 09) Le dirigeant assume la responsabilité de la sécurité de l'information au sein de son entité.

> *Je suis responsable de ça et bien évidemment, de la sécurité de données puisqu'on manipule des données sensibles, on manipule pour le coup des données clients. Avec leur adresse, avec leur numéro de téléphone. Et donc, il faut être extrêmement vigilant sur cette utilisation. (Dirigeant UI, EN 10)*

Le rôle du dirigeant est de déployer la politique et les mesures de sécurité de l'entreprise dans son entité. Par ailleurs, il garantit le respect de toutes les exigences (lois, réglementations, directives nationales) s'appliquant aux activités de l'entreprise ou, plus particulièrement, au domaine métier. Ainsi, les entités de réseau doivent se mettre en conformité avec les exigences de l'Autorité de régulation des télécoms (ARCEP[2]).

Du fait d'un travail quotidien avec les données sensibles, la gestion des risques informationnels est un « sujet essentiel » pour le dirigeant. Au moment de la prise de ses fonctions, il s'engage, entre autres, à protéger toutes les informations, avec une vigilance particulière pour les données confidentielles et personnelles. Le dirigeant doit s'assurer que les mesures de sécurité de l'information sont adéquates par rapport au contexte métier et aux exigences en vigueur. Quand cela n'est plus le cas, il doit entreprendre des actions nécessaires pour les faire évoluer. Un exemple récent concernait le nouveau Règlement Général sur la Protection des Données (RGPD). Pour les dirigeants, ce règlement s'est traduit par l'élaboration d'un plan d'action et de nouvelles mesures de mise en conformité.

La sécurité fait partie des activités du dirigeant et de ses rôles informationnels. Il s'agit d'une problématique d'actualité qui demande des efforts importants : « Aujourd'hui il y a un très gros travail sur la sécurité de la donnée. » (Dirigeant UI, EN 09) C'est un sujet qui concentre l'attention des dirigeants et demande leur implication.

Sécurité de l'information et gestion des risques

Le domaine de réseau comprend un travail fréquent sur le terrain. En conséquence, les acteurs sont équipés des dispositifs numériques portables et des accès déportés au système d'information. Ceci est aussi vrai pour les dirigeants des unités de réseau, très souvent en

[2] L'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) est une autorité administrative indépendante chargée de régulation des marchés des communications électroniques.

mobilité : « je ne suis pratiquement jamais à mon bureau » (Dirigeant UPR, EN 22). Compte tenu de ces conditions, les informations dont ils disposent peuvent faire l'objet d'actions malveillantes. Ainsi, parmi les principaux risques perçus par les dirigeants de réseau figurent : perte ou vol de l'information, risque de piratage, et comportement à risque.

La gestion de ces risques implique d'abord la mise en place des mesures techniques. « Le challenge » est de prévenir la perte de l'information due aux problèmes techniques. Il s'agit aussi d'assurer la protection des informations en cas de vol ou de perte du dispositif de travail : « On a beaucoup de PC portables avec le risque évidemment de s'égarer, soit de se faire voler et ainsi de suite. » (Dirigeant UI, EN 12) En plus de ces causes diverses de perte d'informations, le contexte numérique comporte le risque de piratage et donc de fuite des données. Les possibilités de piratage sont nombreuses « dans le monde digital » et ce risque est considéré comme un « souci majeur » qui doit être maîtrisé et « mis sous pilotage ».

> *Pour l'instant, je pense qu'on est un peu encore émerveillés par les capacités des outils. Et, on va être de plus en plus confronté aux problématiques potentielles de piratage. (Dirigeant UI, EN 16)*

Le dernier risque évoqué par les dirigeants est le comportement à risque. Certains comportements des acteurs peuvent conduire à des dommages involontaires et nuire à l'entreprise. Dans l'exercice de leurs activités, le réflexe sécuritaire n'est pas forcement présent chez les acteurs : « je ne suis pas convaincu que dans le feu de l'action opérationnelle on pense à ce sujet-là. » (Dirigeant UI, EN 16) Un exemple de ce type de risque concerne l'utilisation d'une application externe (WhatsApp) pour échanger des informations. Quand l'usage reste "basique" (ex. se donner un rendez-vous pour le déjeuner) le risque est mineur ou inexistant. Cependant, le dirigeant cite un exemple du niveau technique où l'usage de ce dispositif pour échanger des informations peut avoir des impacts forts : « Si je fais une configuration de routeur chez un client et que ce client c'est une banque, si elle est piratée, vous imaginez ce que ça peut donner » (Dirigeant UI, EN 16). Ce type de comportement ouvre la voie aux menaces comme la divulgation, le vol des données, etc. Pour les maîtriser, une prise de conscience de chacun et une vigilance particulière sont nécessaires dès lors que les informations ou les dispositifs de travail sont utilisés en dehors de la zone sécurisée. Dans cet objectif, le dirigeant détermine des mesures nécessaires de sensibilisation, de formation et de rappel des risques encourus à ses collaborateurs. Toute la difficulté consiste à changer des habitudes et faire évoluer l'usage existant. Alors, la démarche des dirigeants consiste à proposer des alternatives (ex. Skype entreprise) d'un niveau de sécurité satisfaisant.

Pour les dirigeants, la sensibilisation demande une continuité. Les nouveaux acteurs doivent intégrer la démarche dès leur arrivée et comprendre qu'il y a « des droits et devoirs en termes d'utilisation d'information ». Cela permet de développer des comportements sécuritaires durables. En plus des mesures de sensibilisation, l'appui principal au dirigeant dans la démarche de gestion des risques informationnels sont des mesures techniques (cryptage, identifications et accès contrôlés, etc.). Ces « verrous » techniques sont jugés nécessaires pour éviter de « se faire déborder par l'innovation » (Dirigeant UI, EN 16).

Sécurité de l'information versus accès à l'information

La gestion de la sécurité de l'information implique que l'accès au système d'information soit contrôlé et réservé aux personnes habilitées. D'ailleurs, il n'est pas possible d'accéder aux informations à distance si le dispositif utilisé (PC, tablette, téléphone portable) n'est pas doté

d'un système de sécurisation satisfaisant (ex. un VPN[3]). La mise en œuvre de ces mesures fait que, dans certains cas, la sécurité est vécue comme une contrainte (technique, fonctionnelle, organisationnelle).

Le dirigeant attire l'attention sur un « état de fait » à prendre en compte : « c'est plutôt un frein au tout numérique, parce que comment j'accède aux systèmes d'information d'Orange ? » (Dirigeant UI, EN 08) Un exemple concret concerne le traitement des mails et leur chiffrement à l'aide d'une clé PKI[4]. Pour traiter des informations sensibles ou confidentielles, le dirigeant doit utiliser ce système de protection. Cependant, cela signifie que l'information sécurisée est accessible uniquement dans les conditions prédéfinies obligeant l'acteur à réajuster son comportement.

> *On est obligé de travailler de plus en plus avec des mails sécurisés qui sont chiffrés, qui ne sont visibles qu'avec une clé PKI. Je ferais bien 80 % de mes mails depuis mon téléphone si je pouvais, mais tous ces mails-là, aujourd'hui, ils sont lisibles que sur un PC. (Dirigeant UI, EN 08)*

Dans le cas des activités externalisées (sous-traitance), la sécurité de l'information devient un sujet d'ordre organisationnel et contractuel. Le respect des exigences réglementaires et de la confidentialité des informations impose aux partenaires un accès sélectif et limité au système d'information. De plus, le système informatique complexe (constitué d'une myriade d'applications) et initialement conçu pour les salariés d'entreprise rend la gestion et l'attribution des droits d'accès encore plus difficile. Pour pallier ces problèmes d'indisponibilité de l'information, les dirigeants mettent en place d'autres solutions, moins « agiles », demandant parfois des efforts ou des coûts supplémentaires.

Il en ressort que la sécurité de l'information s'impose comme un élément de premier ordre de la praxis des dirigeants et, notamment, dans la définition des droits d'accès à l'information.

DISCUSSION ET CONCLUSION

Ce travail avait pour objectif d'étudier le rôle et les comportements des dirigeants de réseau télécom face aux risques informationnels. L'étude empirique a été menée selon les méthodologies de construction de sens de Dervin et de la théorisation enracinée.

Les résultats de notre étude montrent que le dirigeant de réseau endosse le rôle de responsable de la sécurité de l'information. Ce rôle comprend le déploiement de la politique de sécurité de l'information de l'organisation au sein de son entité, la mise en œuvre des mesures de gestion des risques informationnels et leur évolution en fonction des changements de l'environnement. Ce résultat confirme le travail de Berthevas sur le rôle clé du management au niveau local quant à la stratégie de l'organisation et ses valeurs en termes de gestion des risques informationnels [6]. Ainsi, le dirigeant de réseau organise les activités et les ressources humaines de manière à garantir le respect des exigences. Il veille sur les usages des dispositifs et des informations, sensibilise son personnel et instruit des comportements conformes aux politiques de sécurité. Ces activités correspondent aux activités managériales en lien avec la sécurité de l'information proposées par Williams [20] : développement de la politique en fonction des besoins "métier", implémentation des mesures adoptées, surveillance, sensibilisation et formation, etc. Les résultats de notre étude contribuent aux travaux existants en confirmant que l'activité de gestion des risques informationnels fait partie

[3] Virtual Private Network (VPN) est un système de sécurisation des informations permettant à l'acteur d'accéder à un réseau à distance et en toute sécurité.

[4] Public Key Infrastructure ou Infrastructure à Gestion de Clé comprend des certificats permettant des services d'authentification et de chiffrement des données (interne Orange).

du travail managérial des dirigeants télécom. De ce fait, nous pouvons considérer que le rôle de responsable de la sécurité de l'information fait partie des rôles informationnels des dirigeants présentés dans la catégorisation de Mintzberg [21].

La gestion des risques informationnels est un sujet d'importance majeure pour ces acteurs outillés de nombreux dispositifs numériques. Les risques informationnels perçus par les dirigeants peuvent être classés selon les catégories définies par Loch et al. [22]. Les risques internes à l'organisation concernent des problèmes techniques pouvant causer une perte ou une altération des informations. Les risques externes à l'organisation se traduisent par des actions malveillantes (piratage, vol). D'ailleurs, ces deux catégories de risques (internes et externes) incluent aussi le comportement humain.

Dans certaines situations de travail, les exigences en matière de gestion des risques informationnels et de la sécurité de l'information sont perçues comme des contraintes (fonctionnelles, organisationnelles, techniques). Elles modifient les comportements des acteurs et leurs usages des dispositifs numériques. Ainsi, l'accès aux informations et leur traitement devrait être opérés dans des conditions de sécurité satisfaisantes. Ce résultat complète le travail de Lekic et Lezon Rivière [23] attestant l'influence des exigences sécuritaires sur le partage de l'information dans l'environnement numérique.

Les résultats de notre étude s'accordent avec les travaux précédents démontrant l'importance des efforts et du travail fournis par les dirigeants dans la démarche de gestion des risques informationnels. Ils dévoilent également l'aspect contraignant que la sécurité de l'information peut représenter dans un domaine opérationnel. Cependant, cette étude comprend des limites dues au fait qu'elle se concentre uniquement sur les dirigeants d'un domaine très précis, celui du réseau télécom. De plus, l'aspect sécuritaire n'était pas le focus de notre recherche. Il fait partie d'un périmètre d'étude plus large portant sur l'ensemble des comportements informationnels des dirigeants de réseau. De ce fait, un retour sur le terrain permettrait d'approfondir le travail déjà effectué. Les risques informationnels gagneraient à être étudiés de la perspective d'autres acteurs des entités de réseau télécom. Par ailleurs, l'étude pourrait se poursuivre avec les dirigeants d'autres niveaux de responsabilités et domaines métier.

BIBLIOGRAPHIE :

1. Castelo Branco, G. and M. Bolliger, *Gestion des risques informationnels dans les organisations*. 2018, Haute École de Gestion de Genève (HEG-GE): Gèneve. p. 74.
2. Orange, *Politique de Sécurité Globale pour le Groupe Orange*. 2017, interne Orange.
3. Vallès, L. *Le risque informationnel et l'urgence de le gérer de façon adéquate*. 2015 [consulté le 18/03/2019]; Available from: http://lyonelvalles.com/2015/12/20/le-risque-informationnel-et-lurgence-de-le-gerer-de-facon-adequate/.
4. Léger, M.-A., *Introduction à la gestion de risque informationnel*. 2013, Québec, Canada: CRHOMA.
5. AFNOR, *NF ISO/CEI 27005 : Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information*. 2013, AFNOR: Saint-Denis, France. p. 1-77.
6. Berthevas, J.-F., *Management des réseaux personnels et de la sécurité de l'information dans une perspective d'innovation : le rôle de la culture organisationnelle*. 2013, Université Aix-Marseille. p. 373.

7. Tsohou, A., M. Karyda, and S. Kokolakis, *Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs* Computers & Security, 2015. **52**: p. 128-141.

8. Abraham, S., *Information Security Behavior: Factors & Research Directions*, in *Proceedings of the Seventeenth Americas Conference on Information Systems*. 2011: Detroit, Michigan. p. 1-13.

9. Stewart, H. and J. Jürjens, *Information security management and the human aspect in organizations.* Information and Computer Security, 2017. **25**(5): p. 494-534.

10. Posthumus, S. and R. von Solms, *A framework for the governance of information security*. Computers & Security, 2004. **23**(8): p. 638-646.

11. Ghernaouti, S. and C. Aghroum, *Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité.* Sécurité et stratégie, 2012. **11**(4): p. 74-83.

12. Institute, P., *Closing security gaps to protect corporate data: a study of US an European organisations*. 2016, Ponemon Institute. p. 1-11.

13. Williams, P., *Executive and board roles in information security.* Network Security, 2007. **2007**(8): p. 11-14.

14. Hu, Q., et al., *Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*: Managing Employee Compliance with Information Security Policies.* Decision Sciences, 2012. **43**(4): p. 615-660.

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

16. Kollár, C. and J. Poór, *Organisations in Digital Age–Information Security Aspects of Digital Workplaces*, in *Management, Enterprise and Benchmarking in the 21st Century*. 2016: Budapest. p. 73-82.

17. Soomro, Z.A., M.H. Shah, and J. Ahmed, *Information security management needs more holistic approach: A literature review.* International Journal of Information Management, 2016. **36**(2): p. 215-225.

18. Guillemette, F., J. Luckerhoff, and J.p. Corbin, *Méthodologie de la théorisation enracinée : fondements, procédures et usages*. 2012, Québec: Presses de l'Université du Québec. 282.

19. Dervin, B., *Interviewing as Dialectical Practice: Sense-Making Methodology as Exemplar*, in *International Association for Media and Communication Research (IAMCR)*. 2008, IAMCR: Stockholm, Sweden.

20. Williams, P., *Information Security Governance.* Information Security Technical Report, 2001. **6**(3): p. 60-70.

21. Mintzberg, H., *Chapter 2: The Nature of Managerial Work*, in *The Nature of Managerial Work*. 1997, Pearson. p. 19-41.

22. Loch, K.D., H.H. Carr, and M.E. Warkentin, *Threats to Information Systems: Today's Reality, Yesterday's Understanding.* MIS Quarterly, 1992. **16**(2): p. 173-186.

23. Lekic, D. and A. Lezon-Rivière, *Pratiques de partage de l'information dans l'environnement numérique : cas des dirigeants du réseau télécom.* AIDAinformazioni, 2018. **36**(3-4).