Observatoire des Valeurs
de la Société et du Management

Sécurité de l'information sensible

Comment les crises actuelles en clarifient les dimensions

Livre blanc de la recherche OVSM 2022-2023

Michelle Bergadaà, Ph.D.
Fatima Gueroui, Ph.D.
Jean-Patrick Marquet

1er octobre 2023

Sécurité de l'information sensible - Comment les crises actuelles en clarifient les dimensions

Association OVSM - Observatoire des Valeurs de la Société et du Management.

Photo de couverture : *Séance OVSM de choix du thème de recherche*, Daniel Delmas.

Genève, 1er octobre 2023.

Remerciements

Remercions les dirigeants qui ont reçu en 2023 nos étudiants en entretien et qui nous soutiennent dans nos recherches depuis des années :

Raynald Aeschlimann, Harry Allegrezza, Jacques Apothéloz, Argi Arroyo, David Azagury, Serban Badic, Leyla Baghirzade, Christophe Barman, Jean-François Beausoleil, Philippe Bentele, Yves Berchten, Denis Berdoz, Francesco Bertinelli, Ronan Bigueur, Maxime Borros, Gérald Brandt, Anthony Caffon, Marc Châtelain, Charles Chaussepied, Céline Cheval, Luis Clara-Fernandes, Christian Cramer, Marc Devillard, Frédéric Devillard, Franck Didi, Marco Ferrara, Olivier Ferrari, Giuseppe Flammia, Philippe Gendret, Sylvia Gil, Bertrand Grillon, Philippe Gurtler, Mark Hawkins, Jacques Hertzschuch, Cédric Hyde, Bernard Jaccard, Marcin Jasiak, Robert Jones, Stéphane Jotterand, Gaëlle Jourdan Oury, Marin Katchamakov, Sébastien Klein, Raffi Henri Krikorian, Tony Lefebvre, François Leyss, Stefan Lüders, Fulvio Maccarone, Monica Malcarne, Jean-Patrick Marquet, Carlos Moreira, Vincent Mottet, Serge Natarajan, François Note, Sébastien Oulès, Thierry Outin, Giorgio Pauletto, Joëlle Payom, Philippe Peverelli, Bertrand Rajon, Lanto Rakotoarisoa, Olivier Rigot, Tal Schibler, Jean-Marc Thévenaz, Gabriele Thiede, Félix Urech, Stefano Vaccaro, Laurent Vianin, Jérôme Von Burg, Pascal-Henri Vuilleumier, Mario Werren, Yves Zieba, Timon Zimmermann.

Remercions également les étudiants de Bachelor de l'Université de Genève, membres de la Junior Entreprise Genève, qui ont réalisé, sous la direction de Flavien Jean, les longs entretiens avec les dirigeants : Abaigh Flaherty, Malorie Blumlein, Jessica Gregori, Karolina Lakomska, Philippe Kossilov, Cesare Lombardo, Brune Lonardi, Hassan Mahieldein, Mathieu Tournier, Elia Sanjuan, Gabriel Schmidt, Kenzo Vallat, Chloé von Arx.

Avant-propos

Créé en 1999 sous le nom Observatoire des Valeurs de la Stratégie et du Marketing, l'OVSM nait comme un espace de rencontre entre les trois mondes économique, académique et pédagogique. En 2016, il se transforme en Association indépendante à but non lucratif, sans affiliation politique ni religieuse, et adopte, en 2022, la dénomination « Association OVSM - Observatoire des Valeurs de la Société et du Management ».

Aujourd'hui, notre société savante compte, outre plus d'une trentaine de membres individuels cotisants et très impliqués, 8 membres institutionnels et une relation stable avec plus d'une centaine de hauts dirigeants. Ceux-ci apprécient notre démarche de créateur de rencontres et de connaissance selon le processus de recherche-interaction mis en œuvre par l'OVSM (*cf.* Annexe 1 – Étapes chronologiques de la recherche-interaction de l'OVSM).

Le « Core Concept » de l'OVSM, sa seule raison d'être depuis sa création, est la création de connaissance prospective. L'équation de l'OVSM « Enjeux de société <=> Mutation des savoirs + Employabilité » est le fil rouge de tous les projets d'enseignement et de recherche de l'OVSM. Tout projet de développement, soumis au Bureau de l'OVSM, doit être en mesure de démontrer sa contribution au renforcement de ce « Core Concept » ancré à l'interface des 3 univers : étudiants, entreprises, chercheurs. Ce que représente d'ailleurs son logo.

Site internet : https://ovsm-unige.ch/association-ovsm.html

LinkedIn : https://www.linkedin.com/company/ovsmgeneve/?viewAsMember=true

Table des matières

Introduction

Le caractère distinctif de l'OVSM, ce qui assure sa pérennité depuis plus de trente ans, est la synergie entre des acteurs des mondes économique et académique et le développement de son concept original.

Les deux ancrages de l'OVSM sont d'une part la pédagogie et, d'autre part, la recherche.

• La pédagogie permet de développer des concepts uniques comme le cours de Bachelor « Projets Responsables », qui a reçu le Grand Prix de l'Innovation Pédagogique 2019 de la Conférence internationale des Dirigeants des institutions d'Enseignement supérieur et de recherche de Gestion d'Expression Française (CIDEGEF), de la Fondation nationale pour l'enseignement de la gestion des entreprises (FNEGE) et de l'Agence Universitaire de la Francophonie (AUF). Aujourd'hui, sous la responsabilité du Dr Samad Laaroussi, cet enseignement interfacultaire est un des joyaux de l'OVSM.

• La recherche est le deuxième ancrage de l'OVSM. En recherche, il est commun de dire que l'orientation de la recherche détermine les méthodes qui seront utilisées. Il existe quatre types de recherches.

a) La recherche de solutions à un problème défini réalisée par les chercheurs des entreprises de conseil, dont l'objet est de proposer un modèle normatif et la mise en œuvre d'une pratique spécifique à la situation étudiée. L'orientation action se conclut par la prise de décision par les acteurs du terrain. Les chercheurs de l'OVSM n'ont jamais pratiqué ce type de recherche, puisqu'ils ne sont pas des consultants.

b) La recherche théorique, réalisée par des scientifiques dans le cadre de leurs laboratoires et facultés, dont l'objet est de proposer une nouvelle manière d'éclairer les connaissances. Ces recherches théoriques sont menées par des « pairs » universitaires et leurs résultats sont publiés dans des revues académiques à usage du monde scientifique. L'OVSM ne publie pas ses travaux par cette voie.

L'OVSM a donc investi, depuis sa création, dans les deux autres types de recherche :

c) La recherche managériale opérationnelle où il s'agit de reconstruire la représentation d'une réalité du terrain pour instaurer de nouvelles stratégies et/ou relations organisationnelles. Ici les chercheurs, en communication étroite avec les dirigeants d'entreprises, induisent du terrain une construction organisée et formulent leurs propositions dans les faits comme dans la théorie pour valider leurs propositions.

> Depuis 2005, un nombre restreint de hauts dirigeants se réunit pour débattre ensemble d'une thématique commune, dans le cadre d'un séminaire résidentiel de deux jours et demi. Le séminaire est introduit par la conférence d'un expert international du thème retenu, puis donne lieu à des discussions entre participants. Il permet de faire émerger des propositions au niveau des pratiques individuelles des dirigeants comme des organisations dont ils ont la charge. Les thèmes de recherche traités ont, par exemple, été : *Future of Work, Le manager au défi des mutations structurelles* (2022), *Entre urgence climatique et rentabilité, entre continuité et disruption : quelles décisions pour le dirigeant ?* (2021), *Comment le*

numérique impacte les rythmes temporels du dirigeant ? (2020), *L'éthique du dirigeant à l'âge du numérique* (2019), etc.

d) La recherche académique conceptuelle où il s'agit pour les docteurs de l'OVSM d'ancrer leurs travaux dans un thème prospectif et de proposer les liens entre les observations qui déterminent la dynamique du modèle découvert. Ce dispositif est toujours articulé sur une revue de littérature qui précède le choix de la méthode, la définition de l'échantillonnage et l'induction à proprement parler du modèle conceptuel.

> Depuis la création de l'OVSM, en 1999, et grâce à son financement par de grandes entreprises sponsors, ce type de recherche conceptuelle a permis à de nombreux doctorants de soutenir de brillantes thèses, à des chercheurs invités de rejoindre notre laboratoire, et de publier plus de 200 articles dans des revues académiques, de présenter leurs travaux dans de nombreuses conférences internationales. Ces recherches ont pu se déployer en toute *liberté académique*, car il était inscrit dans la charte de l'OVSM Art 14 : *La professeure Bergadaà et les membres de son équipe sont seuls juges de la réalisation des recherches qui leur semblent les plus prometteuses dans le cadre du laboratoire de l'OVSM.*

Ces deux types de recherches - managériale opérationnelle et académique conceptuelle - conduites par l'OVSM ne sont plus indépendantes aujourd'hui : depuis la création de l'*Association OVSM* en 2016, sous le statut d'association, la thématique annuelle leur est en effet commune. Tout au long de l'année universitaire, professionnels et chercheurs de l'OVSM ont de multiples occasions de se rencontrer et d'échanger leurs points de vue. Dès qu'un thème paraît intrigant aux uns comme aux autres, une étude spécifique est décidée.

Ces deux types de recherche ne sont pas en concurrence, bien au contraire. Elles sont de natures distinctes. Elles n'appellent pas les mêmes compétences de leurs réalisateurs et se complètent. C'est cette synergie qui fait la particularité unique de l'OVSM d'aujourd'hui.

Cette logique de création commune de savoir fondée d'une part sur la recherche managériale opérationnelle réalisée lors du « Séminaire dirigeants » annuel et, d'autre part sur la recherche académique conceptuelle réalisée tout au long d'une année universitaire, éclaire désormais, année après année, des thématiques primordiales sous deux angles complémentaires.

Ceci est particulièrement bienvenu à une époque de bouleversements économiques, politiques, sociaux et bien sûr éducatifs.

Le thème retenu pour 2022-2023 « Sécurité de l'information sensible. Comment les crises actuelles en clarifient les dimensions » appelle ainsi à être appréhendé selon ces deux perspectives vu l'accélération de ses transformations et les nouveaux contextes de travail.

La méthodologie de recherche annuelle se déploie en trois étapes :

1) La mise au point du **guide d'entretien** qui sert de base aux étudiants qui réalisent les interviews des hauts dirigeants d'entreprise. Tous les membres de l'OVSM, chercheurs et managers, se donnent rendez-vous pour élaborer ce

guide d'entretien fruit de débats collectifs. Ces débats ont lieu au cours des repas thématiques à l'auberge La Mère Royaume de Genève, dirigés par le Secrétaire général de l'Association, Daniel Delmas, Dr.-Ing. Le guide d'entretien de l'année 2022-2023 en résultant figure en annexe 2.

2) **La recherche managériale opérationnelle** constitue la partie I de cet ouvrage. Durant le « Séminaire dirigeants » annuel, deux groupes de focus de 8 à 9 participants chacun travaillent sous l'animation de Bertrand Rajon et de Jean-Patrick Marquet, co-présidents de l'Association. L'avantage des groupes de focus est de permettre à un débat animé et aux significations sous-jacentes du thème, d'émerger. Cette méthodologie de groupes de focus est utilisée dans les recherches exploratoires pour mieux cerner la problématique étudiée. Cette première analyse exploratoire par groupe de focus est présentée. Puis, l'avis d'un expert international du thème, Louis-David Magnien, est sollicité à son propos et figure également dans cette partie.

3) **La recherche académique conceptuelle** de l'OVSM constitue la partie II de cet ouvrage. Fondée sur une approche ethnométhodologique, elle permet d'extraire des données, recueillies par des étudiants-interviewers au cours de 70 entretiens de longue durée, une structure et une dynamique de la thématique. Cette recherche conceptuelle a été réalisée par la Dre Fatima Gueroui qui avait été formée à la méthode de recherche par la Prof. Bergadaà. Les résultats de cette analyse, leur synthèse et les perspectives d'approfondissement sont présentés en partie II de cet ouvrage.

Le lecteur découvrira en parcourant nos deux recherches effectuées de manières totalement indépendantes l'une de l'autre leur complémentarité et leur synergie. La recherche managériale opérationnelle dresse le panorama de la perception du thème de la sécurité de l'information qu'ont deux groupes de dirigeants réunis durant une journée complète et dont le riche débat ouvre le champ des possibles. La recherche académique conceptuelle présente une analyse rigoureuse de l'état des lieux en matière de publications scientifiques sur le thème de la sécurité de l'information, puis cerne par une méthode structuraliste avec précision les variables clés du modèle induit des analyses individuelles effectuées de manière tout à fait indépendante sur un échantillon de notre population cible : les dirigeants d'entreprises suisses romandes.

Partie I
Recherche managériale opérationnelle

Chapitre 1
Synthèse des groupes de focus de dirigeants de l'OVSM

1.1 Introduction

La méthodologie des « focus groups » est utilisée dans les situations où le concept étudié est nouveau, mais sur lequel les participants peuvent émettre des opinions. Fortement ancré sur le concept de motivations individuelles, le débat permet de voir émerger aussi bien des tendances à l'action que des freins à la motivation (Stewart *et al.*, 2007[1]). Les Focus groups sont utilisés dans les champs de recherche où la méthode interactionniste s'impose pour déterminer les influences réciproques des agents. L'OVSM réalise chaque année, depuis 1999, des séminaires sous forme de tels groupes de focus.

Les 23 et 24 mars 2023, deux groupes de huit dirigeants membres de l'OVSM se sont réunis au centre de formation international de Nestlé, près de Vevey, pour débattre du thème « Sécurité de l'information » au regard de leurs expériences respectives dans les affaires et la direction des entreprises.

La synthèse des réflexions de ces deux groupes de focus permet de constater que le thème « Sécurité de l'information » recouvre de multiples problématiques dont bien sûr la cybersécurité, sujet central, mais également divers sujets périphériques qui dépassent la question des technologies de l'information. En d'autres termes, il s'agit d'un thème similaire à un iceberg avec une partie émergée et une partie immergée, la première sautant aux yeux, la deuxième moins évidente, mais encore plus considérable dans ses enjeux et risques.

Ainsi, la partie émergée de l'iceberg est la cybersécurité, enjeu majeur des technologies de l'information qui sont au cœur de tous les processus de décision des entreprises. Pour les dirigeants, la cybersécurité recouvre de multiples défis d'architecture informatique, de cryptage, d'authentification, de systèmes « anti », de gestion d'accès, de travail à distance (maison ou mobile), d'évolution technologique (informatique quantique, intelligence artificielle, etc.). Le sujet est technique, d'une complexité croissante, et dépasse souvent les capacités des dirigeants qui se reposent pour sa gestion sur des départements dédiés (dans les grandes entreprises) ou des sous-traitants hautement spécialisés (pour les petites et moyennes entreprises).

Mais, sous cette partie émergée se cache toute une arborescence de tenants et aboutissants de la sécurité de l'information pour une entreprise qui forme une vaste partie immergée : le contrôle des sources d'information, l'intégrité de l'information, la qualité de l'information, le maillon faible humain, les implications de formation et d'éducation, les implications sociétales de la collecte, de l'utilisation, et de la diffusion d'information, les impératifs réglementaires, etc. Ces différents aspects affectent le management des entreprises bien au-delà des technologies de l'information, y compris

[1] Stewart D.W., Shamdasani P.N., Rook D.W. (2007). Focus Groups: Theory and Practice, *Applied Social Research Methods*, SAGE Publications.

le développement commercial, l'organisation de la production, le suivi des risques, la gestion des ressources humaines, la formation continue, la conformité légale et réglementaire.

Pour les dirigeants, cette problématique de la sécurité de l'information dérive d'un nouveau paradigme dans la vie des affaires s'imposant au dirigeant, crée des opportunités considérables pour l'entreprise avec un corollaire de risque qui exige une organisation adaptée et induit l'émergence d'un nouveau contrat social que le dirigeant doit embrasser et promouvoir.

1.2 Vers un nouveau paradigme de la vie sociale et en entreprise

L'environnement des affaires évolue à mesure des avancées technologiques, des changements générationnels, de la mondialisation (ou du fractionnement du monde) et l'entreprise (ainsi que la société) se trouve donc confrontée à un nouveau paradigme.

Divers facteurs peuvent être cités, liste certainement non limitative :

- *La digitalisation des communications* : le temps du courrier, du téléphone et des archives papier est bien lointain et même l'e-mail, l'ordinateur et le scanner sont en passe de se marginaliser avec l'usage grandissant des messageries instantanées (de type WhatsApp, Slack, Instant Bloomberg et autres) et des signatures électroniques (type DocuSign et autres).
- *La décentralisation du stockage* : l'informatique aussi bien personnelle que professionnelle est de plus en plus dans le nuage (« *cloud computing* ») et accessible sur tous supports (smartphone, tablette, ordinateur) et en tous lieux (via Wifi, 5G, Starlink, etc.), avec la documentation numérisée et stockée dans le cloud (sur AWS, Dropbox, OneDoc, Google Drive pour ne citer que quelques prestataires).
- *L'interaction entre les réseaux privés et publics* : la frontière est de plus en plus ténue et difficile à étanchéifier entre réseau d'entreprise fermé (intranet) et réseaux publics ouverts (par exemple LinkedIn), ces derniers étant souvent utilisés pour du réseautage, du démarchage, de la recherche d'information, voire des échanges « *off* » au grand dam des départements de risque et conformité des entreprises.
- *L'accélération des processus* : avec l'instantanéité des communications et de l'accès à l'information, s'est développée une vitesse de réaction plus grande ainsi que son corollaire, une impatience marquée en cas de réponse tardive. Ainsi, le dirigeant bénéficie de nettement moins de temps de réflexion et doit prendre position sans délai, avec le risque d'une décision insuffisamment considérée. En d'autres termes, la célérité a pris le pas sur la qualité, au risque de compromettre la sécurité de l'information qui est évaluée et la décision qui en résulte.
- *La globalisation des relations et des cultures* : avec la mondialisation (et même avec la tendance au fractionnement qui prévaut dernièrement), l'information ne bénéficie plus de l'homogénéité des décennies précédentes, et reflète de moins

en moins des valeurs partagées. Ainsi, la qualité de l'information s'en trouve potentiellement compromise et prête le flanc aux interprétations erronées.

- *Les différences générationnelles* : les générations actuellement aux affaires, X, Y et milléniales, n'approchent pas la recherche, l'analyse et l'usage de l'information de la même façon, faisant preuve d'une appréhension différente des possibilités offertes par les outils d'aujourd'hui et d'une sensibilité différente aux risques. Cet écart est d'autant plus marqué dans le monde professionnel que les générations X et Y sont pour l'essentiel aux manettes de direction et contrôle tandis que la génération milléniale est celle qui contribue à l'innovation et prendra *in fine* la relève.
- *Les débordements des conflits personnels et sociaux* : une tendance de fond s'est fait jour dans les dernières années avec l'instrumentalisation de l'espace informationnel (internet, réseaux sociaux et information dématérialisée) dans les conflits personnels (par exemple, gestion de la performance, égalité des chances, harcèlement, licenciement) et sociaux (rémunération ou conditions de travail). Ces conflits ne se cantonnent plus à l'espace interne à l'entreprise, mais se retrouvent occasionnellement sur la place publique avec le partage d'information sensible (sur l'entreprise, les dirigeants, les clients) comme moyen de pression ou rétorsion.

Au final, l'environnement informationnel de l'entreprise et du dirigeant a considérablement évolué vers plus d'immédiateté, plus d'incertitude et de brutalité, moins de fiabilité et de filtre qui, ensemble, contribuent à magnifier les enjeux de la sécurité de l'information. C'est là un nouveau paradigme qu'il revient à chaque dirigeant d'appréhender et gérer sans possibilité de s'en affranchir, d'autant moins que ce paradigme engendre pour l'entreprise et les affaires de vastes bénéfices potentiels.

1.3 Corrélation entre les opportunités et les risques de l'information

Quand bien même la sécurité de l'information constitue un défi multiforme pour le dirigeant d'aujourd'hui, l'organisation ne peut ignorer le formidable levier offert par l'information telle qu'elle est disponible pour l'entreprise, ses cadres et employés. Nier ou oblitérer ces bénéfices serait un arrêt de mort pour l'entreprise condamnée à vivoter dans le monde du siècle précédent jusqu'à extinction.

En effet, cette profusion d'information et de moyens de communication forme l'essence de ce début du XXIe siècle et offre des opportunités considérables pour qui sait les utiliser. La preuve en est que les sept plus grandes entreprises américaines emblématiques du secteur technologique (ALPHABET, AMAZON, APPLE, META, MICROSOFT, NVIDIA, TESLA) ont à elles seules représenté près de 90% de la croissance de la bourse américaine au cours de l'année 2023 !

Ces opportunités que le dirigeant doit chercher à récolter résultent des facteurs suivants, chaque facteur restant entaché de son corollaire de risque :

- *Plus de facilité de collaboration interne et externe* : cette communication plate ou désintermédiée au sein des équipes de l'entreprise ou avec les partenaires

permet d'accroître le potentiel d'affaires. Mais en parallèle cette collaboration plus directe entraîne des vulnérabilités aux fuites et aux attaques.

- *Plus de diversité des sources* : l'augmentation du nombre de sources d'information et leur plus grande diversité sont un moteur de créativité et d'innovation que le dirigeant doit encourager. Mais cela induit également une moindre confiance dans l'intégrité de l'information collectée en lien direct avec la moindre homogénéité des sources.
- *Plus grand foisonnement de l'information* : cette capacité à collecter plus d'information en provenance d'un plus grand nombre de sources contribue à un foisonnement d'information offrant une vision plus riche. Mais ce foisonnement entraîne une plus grande complexité d'analyse et une moindre confiance dans la qualité de l'information, l'un dans l'autre résultant dans une moindre fiabilité de l'information de l'entreprise.
- *Plus de capacité de traitement* : l'émergence de l'intelligence artificielle permet de mobiliser des capacités de traitement et analyse jamais observées auparavant donc une réactivité et une agilité accrues pour l'entreprise et son dirigeant. Mais en même temps cette sous-traitance de l'analyse à une « boite noire » (« *black box* ») technologique expose la gouvernance de l'entreprise à des biais non-identifiés voire à des influences cachées ou malveillantes.

Au final le monde plus ouvert, plus divers, plus immédiat, plus sophistiqué dans lequel évolue le dirigeant doit permettre d'amplifier la performance individuelle et collective dans l'entreprise, donc d'améliorer la compétitivité, gage de survie dans un environnement concurrentiel mondialisé. Néanmoins ce surcroît de sophistication implique une plus grande complexité au regard des risques induits et ceux-ci requièrent une prise en compte au niveau des équipes (qui doivent se former pour agir en toute sécurité), du dirigeant (qui doit s'informer, impulser et se faire aider), des instances de gouvernance (qui doivent veiller et encourager) et de la société elle-même (qui doit prendre conscience des implications).

1.4 Prise de conscience de l'impact sociétal de la sécurité de l'information

Garantir la sécurité de l'information tout en récoltant les nombreux bénéfices de sa profusion est donc un effort de longue haleine et de vaste portée qui ne peut réussir sans une prise de conscience collective et un engagement de tous dans un contrat social élargi. A ce titre le rôle du dirigeant est essentiel : il doit à la fois embrasser son rôle sociétal autour de la gestion de l'information et promouvoir une version mise à jour du contrat social qui prenne en compte cet impératif de sécurité de l'information.

Pour le dirigeant, plusieurs axes de réflexion et d'action méritent d'être poursuivis :

- *La théorie du glaive et de la cuirasse* : ce classique de la théorie militaire qui veut que chaque progrès technologique du glaive induit un progrès équivalent de la cuirasse permet de comprendre qu'il n'y a jamais de solution garantie et définitive. La sécurité de l'information exige une veille permanente du dirigeant, aussi bien en termes d'investissement dans les dernières technologies de protection (par exemple authentification renforcée ou biométrique, cryptage

quantique, etc.) que de procédures pour renforcer la qualité et l'intégrité de l'information collectée et utilisée par l'entreprise. De la même manière, cet impératif est renforcé par la forte probabilité de voir les possibilités d'assurer le risque se raréfier au fil du temps. Il en résulte que la sécurité de l'information implique de créer dans l'entreprise et la société une culture informationnelle de la sécurité et non pas de la prise de risque.

- *Le clivage entre acteurs économiques* : une appréhension correcte du risque par le dirigeant suppose de reconnaître que tous les acteurs économiques ne sont pas logés à la même enseigne. Les grands acteurs économiques, grandes entreprises ou multinationales (grâce à leurs équipes dédiées et vastes moyens), sont *a priori* mieux équipés pour faire face au risque que les petits acteurs économiques (qui n'ont guère de moyens autonomes et doivent sous-traiter la gestion du risque). Mais le dirigeant réalise que la chaîne d'affaires et d'approvisionnement est complexe et diverse, mutualisant le risque, et par conséquent personne n'est en sécurité tant que tout le monde n'est pas en sécurité.
- *Le rejet d'une dérive centralisatrice* : de même que le dirigeant comprend la nature mutuelle de la sécurité de l'information, il identifie les carences du modèle centralisé type « *big brother* » où l'Etat prétendrait prendre à sa charge la gestion du risque informationnel et l'entreprise abdiquerait sa responsabilité. Plus le système est centralisé, plus le risque d'une brèche catastrophique est grand, et plus les libertés individuelles sont en péril. C'est bien le rôle du dirigeant de plaider contre un système déresponsabilisant et d'exiger un contrôle démocratique robuste. La sécurité de l'information doit être embrassée par tous et par chacun dans la société.
- *La clé est l'esprit critique* : au final, cette notion de tous et de chacun est primordiale pour garantir une gestion du risque efficace à long terme. C'est donc bien au travers de l'éducation à la source (à l'école et à l'université) et de la formation continue (en entreprise) que se construiront l'esprit critique, le questionnement, le doute, qui viendront renforcer le maillon faible humain.

1.5 Conclusion

Ce thème « sécurité de l'information » qui semble au premier abord particulièrement technique et aride se révèle donc en fait un sujet très vaste qui met en cause l'ensemble des processus aboutissant à la prise de décision du dirigeant. Identification des contreparties, recherche d'information, stockage et analyse de données, définition de stratégie d'entreprise, articulation de la chaîne d'affaires, gestion du risque, formation des talents, veille technologique et organisationnelle, écosystème de gouvernance, etc., nombreux sont les facteurs clé de succès de l'entreprise qui dépendent de la sécurité de l'information.

Au niveau de l'entreprise, face à la transformation de l'environnement et aux changements de mentalité, le dirigeant est confronté à des jugements qui dépassent parfois ses compétences et pour lesquels il doit s'appuyer sur des valeurs et des

personnes pertinentes afin de sortir du dilemme par le haut et y consacrer les moyens nécessaires.

Au niveau de la société, la mutualisation des risques et le rôle de tous et de chacun doivent conduire le dirigeant à se faire l'avocat d'une approche systématique de formation au niveau micro, insistant sur les comportements responsables et vertueux, encourageant l'engagement et la transparence individuelle.

Alors que les opportunités résultant de l'information sont immenses et doivent être récoltées, les risques peuvent être gérés en connaissance de cause et en conscience, notamment conscience que les solutions magiques ou centralisées sont illusoires au mieux, néfastes au pire, et que seule la responsabilité individuelle dûment cultivée pourra garantir au long cours la sécurité de l'information.

Chapitre 2
Synthèse de Louis-David Magnien

Louis-David Magnien est directeur général régional, Europe-Moyen Orient-Afrique, de KROLL, le leader mondial de l'intelligence économique et du conseil en gestion du risque. Basé à Paris, il dirige les équipes en France, Belgique, Luxembourg, Suisse, Liechtenstein, Monaco, Andorre et Afrique francophone.

Il est particulièrement impliqué dans la gestion de crise relative aux opérations financières sensibles, la lutte contre la fraude, la corruption et le blanchiment d'argent, la recherche d'actifs offshore, la défense contre les OPA hostiles, l'influence et la contre-influence dans le cadre de litiges judiciaires ou arbitraux, et la due diligence d'intégrité de haut niveau, en particulier sur les particuliers fortunés (HNWI). Il conseille des institutions internationales, des gouvernements et des institutions publiques, de grands cabinets d'avocats, des institutions financières, des fonds d'investissement et des gestionnaires de sociétés cotées dans des situations sensibles et multi-juridictionnelles.

2.1 Introduction et considérations générales

2.1.1 Informations générales

Le terme sécurité de l'information recouvre un grand nombre de significations diverses et variées. En effet, l'information est à la fois processus et objet. Le processus (recueillir des renseignements sur quelqu'un ou quelque chose) induit l'objet « information », synonyme de donnée. Ainsi la sécurité de l'information c'est autant protéger son canal de partage que l'information en elle-même.

D'un point de vue informatique, la sécurité de l'information peut être définie par l'ensemble des moyens qui permettent d'assurer la protection et l'intégrité des données, sensibles ou non, au sein d'une infrastructure numérique ainsi que détecter, recenser et contrer les menaces. Cela s'inscrit dans une démarche continuelle de remise en cause (*Pentest* : simulation d'attaques afin de mettre en lumière les vulnérabilités, opérations Red team…). En effet, la créativité des pirates, l'évolution des technologies de protection disponibles et la diversification des activités de l'organisation (notamment dans le cadre de fusion-acquisition) sont autant de défis pour les acteurs économiques.

Dans une perspective plus large, la sécurité de l'information recouvre également l'environnement informationnel autour de l'entreprise, la presse, les comptes annuels publiés, les rapports spécialisés, etc. Dans un monde économique intimement connecté ou une polémique sur les réseaux sociaux peut avoir une incidence directe sur les performances économiques de la société, il est important de pouvoir maintenir un « narratif ». Assurer la sécurité de l'information c'est également contrôler l'information qui circule dans le domaine public notamment via ce que partagent les employés : les risques associés peuvent être très divers (*social engineering*, espionnage, compromission de propriété intellectuelle, *data leak*).

Il pourrait également être soutenu que pour assurer la sécurité de l'information il est nécessaire de savoir « bien s'informer », à la fois sur le secteur dans lequel on opère, ses concurrents, mais également sur ses partenaires, interlocuteurs, sous-traitants... Mieux les sociétés sont informées, plus elles sont agiles, adaptables et peuvent prendre les meilleures décisions en temps de crise ou en amont de ces dernières.

2.1.2 Un sujet d'actualité qui s'inscrit dans un contexte sensible

La digitalisation des entreprises s'accélère ces dernières années. Elle se traduit par une dématérialisation massive des systèmes d'information (SI) vers le cloud, l'explosion de l'internet des objets (IoT), l'accumulation des données provenant des utilisateurs dans le *Big Data*, autant de cibles nouvelles pour les cybercriminels. L'information revêt un caractère capital pour l'entreprise, pour sa réputation, sa stratégie et son fonctionnement.

En Suisse, en 2022, le nombre de cyberattaques a augmenté de 61% et 107% pour le secteur de la santé (étude de Check Point 2022). D'après une étude PwC Global Digital Trust Insights de 2020, 59% des entreprises suisses souhaitent augmenter leur budget alloué à la cybersécurité.

Les acteurs économiques et institutions doivent faire face à quatre grands défis :

- **Des attaquants toujours plus performants**

À mesure que les entreprises renforcent leurs systèmes de sécurité, les méthodes des cybercriminels deviennent toujours plus sophistiquées. La manne financière associée au cybercrime est telle que les experts estiment que la cybercriminalité est en train de se structurer en une véritable industrie.

Nous assistons à une sophistication grandissante des attaques avec des technologies facilement accessibles. Les technologies liées à l'intelligence artificielle sont très diverses et permettent une complexification des menaces. De plus, les outils d'attaque et programmes informatiques malveillants sont très accessibles.

Au cours de l'année 2022, une nette croissance des cyberattaques à motivations politiques a été identifiée. Que cela soit des groupes de cybercriminels ou des services de renseignement étatiques, les cyberattaques deviennent des armes de pression. Malgré les révélations sur le programme Pegasus de NSO GROUP en 2021, le secteur des entreprises privées de lutte informatique offensive (LIO) reste très actif avec certains Etats développant une véritable industrie du « *hacking* » privée. Parallèlement à ces acteurs offrant des solutions d'espiogiciels, des entreprises fournissant des prestations de « *hacker-for-hire* » conduisent des activités intenses d'espionnage économique et politique au profit de clients variés.

- **Des attaques coûteuses et sophistiquées**

Parmi 550 organisations interrogées dans le monde entre mars 2021 et mars 2022, le coût moyen d'une cyberattaque sur les données a atteint le montant de 4,35 millions de dollars (étude IBM 2022).

Le coût de ces cyberattaques interroge sur la capacité des groupes d'assurance à véritablement « assurer » le risque cyber. Mario Greco, PDG de ZURICH INSURANCE GROUP (ZIG), lors d'une interview au Financial Times en décembre 2022, estimait que les cyberattaques deviendraient à terme « inassurables ». En France, alors même que le gouvernement essaie d'encadrer l'assurance cyber et incite les entreprises à s'assurer, on assisterait à une contraction, encore légère, du marché de l'assurance cyber. Selon Greco, les gouvernements du monde entier doivent « *mettre en place des systèmes privés-publics afin de gérer les risques cybernétiques systémiques qui ne peuvent être quantifiés, à l'instar de ceux qui existent dans certaines juridictions pour les tremblements de terre ou les attaques terroristes* ». Néanmoins, en février 2023, ZURICH GLOBAL VENTURES, une filiale du groupe ZIG a investi une nouvelle fois dans l'insurtech Canadienne BOXX, proposant des solutions « tout-en-un » combinant notamment cyber protection, détection des menaces, sensibilisation et couverture des coûts liés à un cyber incident.

De plus, l'interconnexion des chaînes logistiques et la sous-traitance généralisée entre prestataires plaident pour un renforcement collectif du niveau de cybersécurité, jusqu'aux plus petites entreprises. En effet, les acteurs malveillants tentent de compromettre des équipements périphériques qui leur offrent un accès plus furtif et persistant aux réseaux victimes c'est-à-dire via : les prestataires, les fournisseurs, les sous-traitants, les organismes de tutelle et l'écosystème plus large de leurs cibles finales.

- **L'insuffisant renforcement des dispositifs**

Si les grands groupes développent des compétences en interne pour répondre à cette menace, les PME/TPE et certains secteurs comme celui de la santé, affichent encore un net retard technologique.

Face à l'augmentation des cyberattaques et leur diversification, en décembre 2022, le gouvernement suisse a décidé la création d'un office fédéral pour la cybersécurité transformant le Centre national pour la cybersécurité en une structure à part entière rattachée au ministère de la Défense. Le but de cet office fédéral est d'assurer la protection de l'administration fédérale, soutenir la population et les acteurs économiques à appréhender les cyberattaques, créer une plateforme unique de signalement, diffuser des informations, avertir les acteurs économiques contre les cybermenaces, et sensibiliser le grand public.

- **Un contexte géopolitique sensible**

L'invasion russe de l'Ukraine est un contexte propice à l'augmentation du niveau de la menace et au développement de l' « *hacktivisme* ». Au cours de l'année 2022, une nette croissance des cyberattaques à motivations politiques a été identifiée. Que cela soit des groupes de cybercriminels ou des services de renseignement étatiques, les cyberattaques deviennent des armes de pression. Il est donc probable qu'on assiste à une croissance des attaques sur la chaîne d'approvisionnement, et sur des événements au retentissement mondial (Coupe du monde de rugby en 2023 et Jeux olympiques en 2024 à Paris).

Comme depuis plusieurs années, les acteurs économiques et administrations font face à des tentatives nombreuses d'espionnage informatique dont les modes opératoires les relient souvent à la Chine.

2.2 Principaux risques et tendances

2.2.1 Les différents types d'attaques

Parmi les attaques les plus communes, on retrouve :

- *Phishing* : incitation à entrer dans un processus relationnel en faisant croire à la personne qu'elle échange avec un tiers de confiance. Représente 80% des attaques.
- *Malware* : logiciel malveillant conçu pour infiltrer ou endommager un système d'information, tel que les virus informatiques, chevaux de Troie, logiciels espions, rançongiciels.
- *Spyware* : logiciel destiné à recueillir des informations à l'insu des utilisateurs, comme des codes ou des contenus. En augmentation dans un contexte géopolitique très tendu. On peut noter une augmentation de la menace APT (pour « *Advanced Persistent Threat* ») : cyberattaque ciblée et prolongée au cours de laquelle une personne non autorisée accède au réseau, reste inaperçue pendant une période importante pour surveiller l'activité du réseau et voler des données.
- *Ransomware* : logiciel malveillant rendant inaccessibles ou inopérantes des fonctions digitales essentielles de l'organisation.

Les technologies liées à l'intelligence artificielle sont très diverses et permettent une complexification des menaces de type fraude au président (et plus généralement d'usurpation d'identité) notamment en lien avec le développement de technologies « *deepfake* » : ChatGPT capable d'écrire comme une personne X ou VALL-E de MICROSOFT capable d'imiter une voix sur la base d'un audio de trois secondes. De plus, grâce à des outils comme ChatGPT, les outils d'attaque et programmes informatiques malveillants deviennent très accessibles.

2.2.2 Les tendances 2022/2023

Comme décrit auparavant, au cours de l'année 2022, on note :

- Une forte croissance des cyberattaques à motivations politiques dans un contexte géopolitique sensible.
- Un brouillage des catégories entre cybercriminels, renseignement privé et étatique.
- Les technologies liées à l'intelligence artificielle sont très diverses et permettent une complexification des attaques.
- Le facteur humain demeure une vulnérabilité interne importante.

Il est noté que les salariés sont souvent un point d'entrée efficace pour les cyber pirates au sein d'une organisation. Du fait de la pandémie de COVID-19, le télétravail s'est massivement développé. En 2021, c'est 38% des PME suisses qui ont mis en place le

télétravail pour tous leurs employés (étude de gfs-zürich mandaté par DigitalSwitzerland). En effet, trop précipité, ce déploiement a pu se faire au détriment de la sécurité. La distance a affecté la vigilance des employés : une étude de Deloitte indique que 25% des collaborateurs en télétravail ont été plus exposés aux menaces de type phishing. Une augmentation des attaques de type « *social engineering* » a également été identifiée. En parallèle des salariés, les personnels extérieurs aux organisations (fournisseurs, partenaires, clients, consultants…) représentent également un risque. La compromission d'un partenaire externe peut entraîner des conséquences directes sur la sécurité informatique ou sur la chaîne d'approvisionnement, par exemple. A ce sujet, le cas de l'entreprise suisse WINBIZ est éloquent. Fin novembre 2022, l'hébergeur de services en ligne inforpo.ch subit une attaque informatique. Pour éviter la contagion, l'entreprise arrête ses serveurs, dont ceux de WINBIZ. 8'800 des 50'000 clients sont alors privés d'accès à leur logiciel de gestion de comptabilité basé dans le « *cloud* » et leur activité est fortement impactée.

2.2.3 Étude de cas : phishing & social engineering

Chaque employé, téléphone, ordinateur, profil sur les réseaux représente un point d'accès pour le crime organisé, qui peut ainsi s'infiltrer, extraire des informations et les exploiter.

Dans cette étude de cas, une salariée en Thaïlande du département finance d'un groupe international a été victime d'un « *romance scam* » : une arnaque au sein de laquelle les cybercriminels jouent les amoureux parfaits durant plusieurs semaines de relation virtuelle, puis réclament de l'argent à celui ou celle qui est déjà charmé(e) ou lui proposent des opportunités d'investissement frauduleuses.

La fraude a commencé lorsque cette employée a reçu un mail indiquant qu'un individu l'avait trouvée très belle sur LinkedIn. Au bout de huit semaines, cette employée réalisait les premières transactions au profit des arnaqueurs. En l'espace de six mois, victime des mensonges et des manipulations des criminels, cette salariée a fini par voler des comptes de son entreprise 250 millions de dollars. Elle a transféré ces sommes vers des dizaines de comptes bancaires dans une vingtaine de pays. Les escrocs inventaient toujours de nouvelles histoires pour l'inciter à effectuer de nouveaux transferts.

Dans cette investigation, les recherches ont permis d'identifier les fraudeurs, les localiser et démonter les nombreuses fausses identités qu'ils avaient construites de toutes pièces (avocat, financier, etc.). Ces derniers avaient enregistré des sites internet d'investissement frauduleux, avaient fait des faux papiers officiels et avaient même organisé des rencontres d'affaires sur place en Thaïlande. Au bout de huit semaines, la salariée réalisait les premières transactions. Plus de 70% (204 millions de dollars) des fonds frauduleux ont été transférés à Hong Kong et à Singapour via des sociétés-écrans. En 18 mois, l'investigation de Kroll a permis d'identifier, geler et au final recouvrer 170 millions sur les 250 millions de dollars.

Dans cette investigation, Kroll a eu accès à différentes sources d'information pour reconstruire chaque étape de la fraude :

- Les comptes bancaires des bénéficiaires des transactions, la date et l'heure de ces transactions et toutes les métadonnées associées.
- Les adresses e-mail d'échanges, messages WhatsApp, discussions sur les réseaux sociaux.
- L'infrastructure Internet et informatique de la société de la victime, y compris les sites web consultés, les points IP de connexion internet, les métadonnées des documents échangés avec les fraudeurs, etc.
- Des sources ouvertes, principalement les réseaux sociaux.

2.3 Comment mitiger ces risques ?

L'augmentation des cyberattaques a participé à la prise de conscience sur la nécessité du renforcement des Directions des Systèmes d'Information (DSI) en interne, ou à l'appel à des prestataires externes pour développer sa résilience cyber, sensibiliser les collaborateurs et diffuser les bonnes pratiques (mise en place de pare-feu, sauvegardes régulières des données, sécurisation du service de messagerie électronique, mises à jour régulières…). Il est également conseillé aux entreprises de mener une veille technologique et réglementaire pour rester informé sur les nouvelles solutions de cybersécurité, les nouveaux types d'attaques informatiques et de s'adapter aux nouveaux règlements, lois et normes.

Ces attaques ne sont pas une fatalité et l'adoption de normes de « cyber hygiène » et d'une sensibilisation généralisée permet de se prémunir des menaces les plus courantes : mise à jour régulière des antivirus, dissociation des messageries personnelles et professionnelles, limitation de l'usage de périphériques pour transférer des données d'un ordinateur à un autre…

L'attention des DSI est souvent portée sur la menace extérieure, mais les données des entreprises peuvent également être compromises par la malveillance des employés. Il peut arriver que certains employés (ou ex-employés) cherchent à placer leur entreprise dans une situation de vulnérabilité, que ce soit à des fins d'espionnage, pour des motivations financières ou par vengeance d'autant plus dans un contexte économique tendu. Environ 21% des entreprises déclarent qu'un employé ayant quitté l'entreprise a déjà transmis des informations importantes à son nouvel employeur (étude de l'agence de détectives LENTZ). Les (ex-)employés malveillants profitent souvent de la négligence interne correspondante. En plus de la prévention, l'entreprise peut contrôler sur le réseau l'effectivité des mesures de prévention, et en même temps détecter toute déviation et dysfonctionnement afin d'y remédier.

2.3.1 Mitiger les risques : la gestion de crise

Pour résumer, les entreprises ne sont jamais à l'abri d'une cyberattaque, il est nécessaire de se préparer aux crises potentielles :

Se préparer à une crise cyber	Mettre en place une stratégie de résilience	Préparer une communication de crise
- Connaître ses actifs et ses services critiques - Renforcer en permanence son SI et l'adapter aux nouvelles menaces *(cf.* veille) - Développer la culture de la cybersécurité de l'entreprise - Audit « pentest »	- Permettre une communication rapide entre les acteurs clés en interne et en externe - Avoir la possibilité d'accéder à des outils hors ligne - Développer un protocole de gestion de crise (et le tester régulièrement via des exercices de gestion de crise)	- A destination des clients, collaborateurs, partenaires, interlocuteurs institutionnels, etc. destinée à rassurer. - Communication avec les agences gouvernementales spécialisées : NCSC pour la Suisse, ANSSI pour la France…

2.3.2 L'apport des nouvelles technologies face à ces menaces

On peut ici porter une réflexion autour de quatre technologies innovantes qui pourraient permettre un renforcement global de la sécurité informatique :

• La fin du mot de passe (« passwordless ») comme clef de voûte de la cybersécurité

L'authentification sans mot de passe est une méthode d'authentification qui permet à un utilisateur d'accéder à une application ou à un système informatique sans avoir à saisir un mot de passe ou à répondre à des questions de sécurité. À la place, l'utilisateur fournit une autre forme de preuve, comme une empreinte digitale, un badge de proximité ou un code de jeton matériel. Il s'agit de sécuriser les usagers des innombrables plateformes en ligne et donc des nombreux mots de passe dont ils se servent pour se connecter, mots de passe souvent trop simples à deviner.

L'authentification sans mot de passe repose sur une paire de clés cryptographiques qui utilise une clé privée (uniquement connue par le propriétaire/l'utilisateur) et une clé publique (pouvant être connue par d'autres). La clé publique est générée lors de l'enrôlement de l'utilisateur au service d'authentification, tandis que la clé privée est stockée sur son équipement (« *device* ») de confiance et ne peut être utilisée qu'en fournissant une preuve d'identité, c'est-à-dire le second facteur (du type empreintes digitales, scans rétiniens, reconnaissance faciale ou vocale). APPLE, GOOGLE et MICROSOFT ont annoncé leur intention d'allier leurs capacités afin de développer une norme de connexion sans mot de passe.

• Le « Zero Trust Architecture »

Le développement du « *Zero Trust Architecture* » (ZTA) comme réponse aux risques cyber divers et particulièrement à ceux liés au télétravail et au BYOD (« Bring Your Own Device ») : ZTA n'est pas une technologie particulière, mais un modèle d'architecture informatique fonctionnant selon le principe de « l'accès au moindre privilège ». En somme, les utilisateurs ou groupes d'utilisateurs ont accès seulement

aux données auxquelles ils ont besoin sans plus et leur accès au réseau et aux données est conditionné par la nécessité de continuellement prouver leur identité. GARTNER, la société de recherche et de conseil technologique basée à Stanford, USA, estime que le secteur des architectures ZTA connaît la croissance la plus rapide des secteurs liés à la sécurité des réseaux et devrait progresser de 31% en 2023. Enfin, l'administration Biden a publié un mémo le 26 janvier 2022 demandant aux agences fédérales d'adopter une ZTA d'ici la fin de l'année 2024.

• L'intelligence artificielle et le « machine learning »

L'IA pourrait apporter des solutions précieuses dans la détection de menaces sur un réseau informatique, de comportements anormaux sur un système, mais aussi d'audit de cybersécurité toujours plus précis (avec l'apprentissage des précédents audits).

• La blockchain

Une alternative décentralisée théoriquement inviolable, accessible par les membres du réseau, pourrait constituer une forme viable de stockage de l'information, ou de sécurisation des infrastructures critiques liées à internet. Un processus de validation cryptographique pourrait accompagner la possibilité d'un individu d'avoir accès à certains types de documents.

Partie II
Recherche académique conceptuelle

Partie II présentée par la Dre Fatima Gueroui

La recherche conceptuelle présentée dans les pages qui suivent a été réalisée par Fatima Gueroui et complétée par Michelle Bergadaà. Fatima Gueroui a obtenu son doctorat de la Faculté de Management et Sciences de la Société de l'Université de Genève en 2007 avec félicitations du jury à l'unanimité et proposition de la publier.

Elle a poursuivi sa carrière par des postes de responsabilité de projets pédagogiques et des travaux de recherche dans plusieurs institutions académiques de Suisse romande (UNIGE, UNIL, HES-SO), puis pour des organisations internationales (OIF, OCDE).

Fatima Gueroui est toujours restée en contact avec l'OVSM et a publié des livres comme Les temporalités du Web, 2014, (avec P.-J. Benghozi et M. Bergadaà), de Boeck University Press, Coll. Le point sur e-business & e-communication et « Les cas de l'Aéroport de Genève », 2014, (avec D. Delmas), Centrale des Cas et des Médias Pédagogiques. C'est donc naturellement qu'elle a pris la relève de Michelle Bergadaà pour diriger les recherches conceptuelles de l'OVSM.

Chapitre 1
Analyse de la bibliographie sur le sujet de recherche

Alors que l'eau puis l'énergie avaient régi les sociétés antérieures (fondées sur l'agriculture puis l'industrie), c'est l'information qui constitue la colonne vertébrale du monde moderne (Ambrosi *et al.*, 2020). En effet, les métamorphoses consécutives de l'économie mondiale ont remodelé l'environnement des affaires, les facteurs clés de succès d'innombrables activités évoluent ainsi d'actifs matériels vers des actifs immatériels, l'information et sa valeur deviennent de plus en plus importantes (Ključnikov *et al.*, 2019) et sont considérées comme des ressources très précieuses (Antunes *et al.*, 2021).

De nos jours, une grande quantité de données complexes est échangée, stockée, transportée (clé USB, *smartphones*) et partagée (5G, WIFI, *bluetooth*) pour des besoins privés et professionnels. Toutefois, la fiabilité de ces données est devenue un enjeu majeur du point de vue de leur sécurisation (Munier *et al.*, 2014). L'ère actuelle des progrès technologiques rapides a permis aux entreprises, d'une part, de reproduire à faible coût et d'améliorer le taux de transmission de l'information, mais, d'autre part, elle a fait peser de nouvelles menaces sur la gestion des informations (Singh *et al.*, 2014 ; Soomro *et al.*, 2016). Les données et l'information sont devenues des cibles potentielles devant être protégées (Ključnikov *et al.*, 2019) d'une variété de menaces provenant de l'environnement organisationnel externe et interne (McFadzean *et al.*, 2007).

La dépendance à l'égard de l'information et des ressources d'information a créé le besoin d'un niveau de sécurité des informations plus élevé (Al-Harethi et Al-Amoodi, 2019).

Les entreprises ont accru leur niveau de conscience concernant la gestion de la sécurité de l'information, car de nouvelles vulnérabilités sont apparues, dans un environnement qui évoluait déjà rapidement, et menacent l'entreprise et ses actifs informationnels (McFadzean *et al.*, 2007). Par ailleurs, l'information a un impact significatif sur le succès des opérations commerciales (Soomro *et al.*, 2016), elle assure la continuité des activités et la confiance des clients (Ma *et al.*, 2009). Sa défaillance peut sévèrement affecter la compétitivité et la survie sur les marchés mondiaux (Antunes *et al.*, 2021). De ce fait, la protection des données et des informations contre les menaces potentielles devrait faire partie de la stratégie commerciale, car le progrès de l'entreprise en dépend (Zaydi et Nassereddine, 2020).

Bien que des solutions techniques soient nécessaires pour protéger les actifs informationnels, elles ne sont pas suffisantes pour relever les défis de la sécurité de l'information dans des environnements sociotechniques complexes et changeants (Holgate *et al.* 2012). La sécurité de l'information n'est plus une alternative, considérée sous une perspective purement technique (Singh *et al.*, 2014 ; Zaydi et Nassereddine, 2020), mais une nécessité légale, éthique et opérationnelle (Al-Harethi et Al-Amoodi, 2019). Relever les défis de la sécurité de l'information dépend fortement des aspects de gestion et de comportement qui sont souvent négligés par les organisations (Singh *et al.*, 2014). Une approche plus holistique, intégrant les éléments organisationnels et humains, est nécessaire pour la recherche sur la gestion de la sécurité de l'information afin de mieux relier les objectifs organisationnels avec leur protection (Soomro *et al.*, 2016 ; AlGhamdi *et al.*, 2020 ; Schinagl et Shahim, 2020).

La gestion de la sécurité de l'information concerne davantage les procédures et processus opérationnels dans lesquels des composants cruciaux tels que l'infrastructure organisationnelle, les facteurs humains et les pratiques de sécurité de l'information sont tous impliqués (Ma *et al.*, 2009). C'est précisément sous cet angle que la recherche OVSM 2023 a été abordée. L'interrogation qui a structuré cette recherche porte sur la compréhension de l'articulation de la gouvernance de la sécurité de l'information face à la nouvelle donne sociétale et environnementale. Plus spécifiquement, l'intérêt a porté sur l'appréhension des enjeux par les dirigeants (dimension individuelle), la structuration des pratiques managériales (dimension organisationnelle) et l'impact de nouvelles exigences sociales (dimension sociétale).

Selon Bergadaà (2020, chap. 3), l'analyse de type structuraliste de ces modèles est toujours simplificatrice de la réalité, mais elle ne serait réductionniste que si des dimensions importantes étaient omises. La réalisation préalable d'une revue de littérature interdisciplinaire évite, *a priori*, le piège de la superficialité. Pour l'auteur, la robustesse du modèle est ensuite qualifiée par le travail de terrain qui apporte des éléments qui l'enrichissent et le précisent ou, au contraire, l'invalident. Ainsi, une revue de littérature scientifique compose le premier chapitre de notre recherche. Elle apporte un éclairage sur les trois dimensions susmentionnées de la gouvernance. Le deuxième chapitre explicite la méthodologie et l'usage des entretiens en profondeur réalisés auprès de 72 hauts dirigeants de Suisse Romande. Notre analyse se focalise sur la perception profonde du top management qui a une responsabilité directe dans la gouvernance de la sécurité de l'information (Von Solms et Von Solms, 2004) et qui constitue ainsi un pilier clé de sa gestion (Hashim et Razali, 2019). Les résultats de ces

entretiens sont ensuite détaillés et discutés. Finalement, le troisième chapitre conclut sur les apports théoriques et pratiques ainsi que les voies de recherches futures.

1.1 Définition de la sécurité de l'information

La sécurité est une situation dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol ou de détérioration[2]. Appliquée aux actifs informationnels d'une entreprise, la sécurité de l'information correspond à la protection de l'information lors de sa création, son traitement, son stockage, sa transmission et son élimination (Khouri, 2009)[3]. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité de l'information au travers de l'application d'une politique, de programmes de formation, d'éveil, de prise de conscience et d'outils technologiques (Whitman et Mattord, 2021). Antunes *et al.* (2021) affirment que la confidentialité est une préoccupation majeure nécessitant l'application d'un ensemble de procédures et de règles au sein de l'organisation (définir qui a accès aux données et aux informations), l'intégrité et la disponibilité se concentrent sur la fiabilité et l'exactitude des données auxquelles accèdent les personnes autorisées.

Plusieurs recherches recommandent le recours au référentiel de pratique COBIT (Control Objectives for Information and Related Technology), au guide NIST 800-100 (National Institute of Standard and Technology) ou à la norme internationale ISO/IEC27001 (éditée par l'International Standard Organisation et l'International Electronic Commission) pour la gestion et la gouvernance de la sécurité de l'information (Scholl, 2018 ; AlGhamdi *et al.*, 2020 ; Schinagl et Shahim, 2020 ; Antunes *et al.*, 2021). Le COBIT est un cadre utile pour la gouvernance (AlGhamdi *et al.*, 2020), il focalise sur le développement de politiques et bonnes pratiques en matière de sécurité de l'information (Hashim et Razali, 2019). Pour le NIST 800-100, il assiste les managers dans l'établissement et l'implémentation de programmes de management de sécurité de l'information (Hashim et Razali, 2019). Par ailleurs, la norme de gestion ISO/IEC27001 définit une liste de contrôle à considérer lors de l'implémentation d'un système de management de la sécurité de l'information (Antunes *et al.*, 2021).

Le système de management de la sécurité de l'information est mis en œuvre afin de réduire les dommages aux actifs sensibles (données financières, documents de propriété intellectuelle, données relatives au personnel ou informations confiées par des tiers)[4], retenir l'information et renforcer la sécurité de l'information (Hashim et Razali, 2019 ; Ključnikov *et al.*, 2019). Il fait partie du système de gestion globale de l'entreprise, fixe l'orientation stratégique en permettant une gestion optimale de risques de sécurité de l'information (Tan *et al.*, 2017). Il regroupe l'ensemble des exigences relatives aux systèmes de management de la sécurité des informations[5]. Il se compose de politiques, de procédures, de lignes directrices, d'activités et de ressources associées, gérées par

[2] *https://www.larousse.fr/dictionnaires/francais/s%C3%A9curit%C3%A9/71792#:~:text=Situation%20dans%20laquelle%20quelqu'un,installation%20pr%C3%A9sente%20une%20s%C3%A9curit%C3%A9%20totale.&text=2.,du%20danger%2C%20qui%20est%20rassur%C3%A9.&text=3*.

[3] *Cité par Ključnikov, Mura et Sklenár (2019)*

[4] *https://www.iso.org/fr/standard/iso-iec-27000-family*

[5] *https://www.iso.org/fr/standard/iso-iec-27000-family*

une entreprise pour protéger ses actifs informationnels (Singh *et al.*, 2014). Il permet ainsi de fixer une orientation stratégique, garantir l'atteinte des objectifs, assurer une gestion appropriée des risques et de vérifier que les ressources de l'entreprise sont utilisées de manière responsable (Tan *et al.*, 2017).

1.2 Définition de la gouvernance de la sécurité de l'information

D'une préoccupation purement technique, la sécurité de l'information est devenue un aspect stratégique et un élément prioritaire pour les entreprises (Schinagl et Shahim, 2020). Bien que l'aspect technologique soit primordial dans le management de la sécurité de l'information, les recherches confirment une nécessaire considération d'une perspective holistique qui prenne en compte la multi dimensionnalité de la sécurité de l'information (Singh *et al.*, 2014 ; Ahlan *et al.*, 2015 ; Soomro *et al.*, 2016 ; Hashim et Razali, 2019 ; Al-Harethi et Al-Amoodi, 2019). Comme ceci sera détaillé dans la section suivante, le facteur humain est l'une des composantes les plus régulièrement mises en avant par ces recherches. Il est en effet indispensable de s'intéresser à la perception et la motivation des collaborateurs et des dirigeants dans le cadre des études sur la sécurité de l'information, car c'est ce qui aide à connaître le type d'actions préventives et réduire les incidents relatifs (Ahlan *et al*., 2015).

Le choix a porté dans le cadre de cette recherche sur une visée stratégique de la sécurité de l'information, cette approche est communément appelée gouvernance de la sécurité de l'information (Dagorn et Poussing, 2012 ; Nicho, 2018). C'est une planification stratégique des responsabilités (Whitman et Mattord, 2021). Elle va au-delà de la garantie opérationnelle de la protection des informations (Dagorn et Poussing, 2012). Elle consiste en l'application des principes de gouvernance organisationnelle (qui correspond à la responsabilité des dirigeants à fournir une direction stratégique, s'assurer que les risques soient correctement gérés avec un usage responsable des ressources) aux actifs informationnels (Whitman et Mattord, 2021).

La gouvernance de la sécurité de l'information regroupe l'ensemble des responsabilités et des pratiques managériales (Tan *et al.*, 2017) qui permet l'alignement des objectifs organisationnels avec les politiques de sécurité de l'information (AlGhamdi *et al.*, 2020). Elle implique une vision holistique du management de la sécurité de l'information, comprenant des enjeux, des décisions, une stratégie globale et à long terme qui ne font pas partie des missions du technicien (Dagorn et Poussing, 2012). Le concept de gouvernance de sécurité de l'information présente des avantages stratégiques multiples (Whitman et Mattord, 2021), il autorise notamment de mieux connecter les objectifs de l'organisation avec sa protection et assurer la continuité de l'évaluation ainsi que la conformité des procédures avec les politiques (AlGhamdi *et al.*, 2020).

1.3 Les défis du dirigeant dans la gouvernance de la sécurité de l'information

La littérature souligne la nécessité d'impliquer la direction au plus haut niveau dans l'élaboration et la mise en œuvre d'une politique de sécurité de l'information efficace (McFadzean *et al.*, 2007 ; Soomro *et al.*, 2016 ; Al-Harethi et Al-Amoodi, 2019 ; Scholl, 2018 ; Schinagl et Shahim, 2020). McFadzean *et al.* (2007) affirment que les

politiques de sécurité doivent être conçues par la direction qui dispose d'une vision holistique permettant l'évaluation de l'organisation et la mise en œuvre en temps opportun des procédures et de systèmes assurant la sécurité de l'information. Par ailleurs, c'est la direction qui contrôle les actifs de l'entreprise et qui a le devoir de fixer des objectifs réalisables en termes de sécurité de l'information en mettant à disposition les moyens *ad hoc* pour y parvenir (Scholl, 2018 ; Al-Harethi et Al-Amoodi, 2019).

Par ailleurs, le leadership et l'engagement du top management sont deux composantes essentielles du succès de l'implémentation du système de management de la sécurité de l'information (Hashim et Razali, 2019). Les auteurs arguent que l'engagement direct du top management facilite l'implémentation du système de sécurité de l'information et motive les collaborateurs à y adhérer. Toutefois, certains facteurs peuvent entraver cet engagement. Schinagl et Shahim (2020) ont plus particulièrement souligné les effets néfastes de la délégation, de la communication et de la contrainte budgétaire : la délégation devient un obstacle majeur quand les dirigeants délèguent la responsabilité aux spécialistes, car ils considèrent qu'ils ne maîtrisent pas suffisamment l'informatique ; l'incapacité des experts à exprimer la nécessité de la sécurité de l'information conduit à une mauvaise communication sur les menaces qu'elle représente ; finalement, le management de la sécurité de l'information est entravé quand cette dernière est considérée comme une dépense plutôt que comme un investissement.

Les dirigeants ont la responsabilité globale de la gouvernance de la sécurité de l'information (Scholl, 2018), ils doivent gérer les aspects non techniques de la sécurité de l'information tels que l'élaboration de la politique de sécurité, la formation, la sensibilisation, l'acquisition de matériel et de logiciels de sécurité, le contrôle interne et les décisions concernant le traitement des données (Soomro *et al.*, 2016). Leur engagement en matière de sécurité de l'information est affecté par des facteurs contextuels organisationnels (type d'industrie, taille, structure) et par les actions stratégiques et opérationnelles réalisées au sein de l'entreprise (McFadzean *et al.*, 2007 ; Soomro *et al.*, 2016). Plusieurs chercheurs ont abordé le management de la sécurité de l'information selon une approche multidimensionnelle (tableau 1 ci-dessous) engageant un processus décisionnel continu (Ma *et al.*, 2009). Les menaces doivent être gérées à chaque étape du cycle de vie de l'information : génération, traitement, stockage et distribution (Singh *et al.* , 2014). Ainsi, une multitude de facteurs affecte la prise de conscience et la gestion des besoins organisationnels en matière de sécurité de l'information (Singh *et al.*, 2014 ; Ahlan *et al.*, 2015 ; Soomro *et al.*, 2016 ; Hashim et Razali, 2019 ; Al-Harethi et Al-Amoodi, 2019).

Tableau 1 : *Les recherches sur les facteurs qui influencent la sécurité de l'information*

	Les recherches et études sur les dimensions de la sécurité de l'information
Singh *et al.* (2014)	Étude qualitative et quantitative pour déterminer les facteurs clés de gestion de sécurité de l'information

	- Les facteurs de niveau **stratégique** incluent le support de la haute direction et la politique de sécurité de l'information. Ces facteurs sont liés à la politique par laquelle les buts et les objectifs de sécurité de l'information d'une organisation sont définis. - Au niveau **tactique**, les facteurs sont orientés *processus* où diverses directives liées aux activités au management de la sécurité de l'information sont développées. Ces facteurs comprennent la formation à la sécurité de l'information, la sensibilisation et la culture de l'entreprise. - Au niveau **opérationnel**, les facteurs sont déterminés par des mesures. Par conséquent, l'audit de sécurité de l'information, la gestion des actifs et les meilleures pratiques de gestion sécurité de l'information sont considérés comme des facteurs opérationnels.
Ahlan *et al.* (2015)	Étude quantitative pour évaluer l'impact de trois catégories de facteurs influant sur la sécurité de l'information : - **Facteurs individuels** (attitude, connaissance et comportement) - **Facteurs institutionnels** (politique et formation) - Facteurs **environnementaux** (performance des pairs, pressions sociales, intention de se conformer et risque perçu)
Soomro *et al.* (2016)	Revue de littérature approche de la sécurité de l'information : - les **facteurs techniques** concernant la planification et l'acquisition de nouvelles technologies, les allocations budgétaires et l'achat de matériel et de logiciels sont à la discrétion de la direction. - Les **facteurs humains**, par exemple la recherche de talents, l'embauche de personnel spécialisé, la formation et la motivation des employés et l'exécution de diverses politiques, sont des responsabilités de gestion sous l'égide du service de gestion des ressources humaines. - Les **facteurs organisationnels**, tels que l'élaboration d'une politique de sécurité, la sensibilisation, la conformité et la mise en œuvre des meilleures pratiques, sont des mesures de base pour la sécurité de l'information.
Hashim et Razali (2019)	Étude sur les facteurs clés de succès de la sécurité de l'information : - Les **facteurs humains** : ont trait au leadership, l'engagement, la connaissance, la communication et la compétence du top management de l'équipe de coordination, l'équipe technique et l'équipe de coordination - Les **facteurs processus** : sont relatifs à la planification stratégique, la mise en œuvre, l'audit et l'amélioration.
Al-Harethi et Al-Amoodi, (2019).	Étude quantitative sur les facteurs concernant les pratiques organisationnelles en matière de **sécurité de l'information** : elle implique de multiples facteurs qui n'ont pas été catégorisés : la

	politique de sécurité, la formation des employés, la protection des « information assets », la communication, le contrôle des accès, la gestion du plan de continuité.

⇨ ***Dans le cadre de cette recherche OVSM, l'intérêt porte sur la compréhension du rôle du dirigeant et la perception qu'il a des dimensions prioritaires de la gouvernance de la sécurité de l'information.***

1.4 Les pratiques organisationnelles de la gouvernance de la sécurité de l'information

L'être humain est souvent qualifié de facteur critique dans les rapports et la littérature sur les processus de sécurité de l'information (Chen *et al.*, 2008 ; Soomro *et al.*, 2016 ; Safa *et al.*, 2016 ; Scholl, 2018). Mais, le comportement des collaborateurs est une arme à double tranchant (Soomro *et al.*, 2016). D'une part, la négligence ou les violations internes des mesures de sécurité de l'information constituent un risque majeur, car elles peuvent entrainer plusieurs abus dont des fraudes, des divulgations non autorisées ou des vols de propriété intellectuelle[6] (Vance *et al.*, 2012 ; Parsons *et al.*, 2014). En effet, le manque de sensibilisation, l'ignorance, la négligence ou la résistance sont à l'origine des manquements internes (Safa *et al.*, 2016). D'autre part, la conformité des employés à la politique de sécurité, la sensibilisation et la formation auront un impact positif significatif sur la sécurité de l'information (Soomro *et al.*, 2016).

Par ailleurs, la gestion de la sécurité de l'information peut être divisée en deux composantes principales, à savoir technique et managériale (Ma *et al.*, 2009), et c'est l'intégration de ces deux aspects qui garantit l'efficacité de la sécurité de l'information (Soomro *et al.*, 2016). En matière de gouvernance, les dirigeants assurent une fonction de modèle, fixent des objectifs réalisables de sécurité de l'information et doivent mettre en place une communication et documentation efficaces (Scholl, 2018). Outre le rôle de management du risque qui constitue une activité cruciale de la gouvernance de la sécurité de l'information (Rashim et Razali, 2019), la littérature aborde diverses pratiques managériales efficaces dans la gestion de la sécurité de l'information (Soomro *et al.*, 2016). Les pratiques les plus discutées sont, selon les auteurs, l'élaboration de politiques de sécurité de l'information, la sensibilisation et la formation des collaborateurs.

Le management de la sécurité de l'information requiert une combinaison de contrôles techniques et procéduraux pour gérer les risques d'information (Kruger et Kearney, 2006). L'analyse constante des menaces auxquelles les entreprises sont confrontées est essentielle pour comprendre l'évolution des stratégies des attaquants et construire des

[6] *Les comportements humains qui peuvent mettre une organisation en danger incluent la divulgation par inadvertance ou délibérément de mots de passe à d'autres, le fait d'être victime de courriels de phishing en cliquant sur des liens de sites Web intégrés ou l'insertion de médias non familiers dans des ordinateurs professionnels ou personnels (Parsons et al., 2014).*

défenses plus fiables (School, 2018). De plus, garantir la sécurité de l'information est intrinsèquement relatif à l'évaluation des risques et des niveaux d'acceptation conçus pour gérer efficacement ces derniers (Singh *et al.*, 2014). Les normes et cadres de sécurité de l'information reposent donc sur la mise en œuvre de politiques et de contrôles pour gérer la sécurité et les risques au niveau organisationnel (Antunes *et al.*, 2021). Les entreprises doivent appliquer en permanence **l'analyse des risques** qui jouera un rôle déterminant dans le maintien des données et la protection de leur système (Al-Harethi et Al-Amoodi, 2019).

La sensibilisation des collaborateurs à la sécurité de l'information est l'un des aspects les plus significatifs dans le domaine et de nombreuses normes et référentiels internationaux (ISO 27001 ou COBIT) mettent en exergue son importance (Rohan *et al.*, 2023). La mise en œuvre de contrôles de sécurité efficaces dépend de la création d'un environnement de sécurité positif, où chacun comprend et s'engage dans les comportements qui sont attendus d'eux (Kruger et Kearney, 2006). La sensibilisation à la sécurité de l'information est indispensable, car elle influence le comportement des collaborateurs, dynamise les activités de sécurité et permet aux entreprises d'être plus réactives face aux menaces (Al-Harethi et Al-Amoodi, 2019).

La sensibilisation à la sécurité de l'information a deux composantes, la première met l'accent sur la mesure dans laquelle les collaborateurs comprennent l'importance des problèmes et des menaces liés à la sécurité de l'information (connaissance et sensibilisation), tandis que la seconde se concentre sur la mesure dans laquelle les utilisateurs respectent les règles de confidentialité et de sécurité des organisations lorsqu'ils utilisent Internet (activités et conformité) (Rohan *et al.*, 2023). Alors que la sécurité de l'information se concentre généralement sur la protection de la confidentialité, de l'intégrité et de la disponibilité des informations, la sensibilisation à la sécurité de l'information traite de l'utilisation de programmes de sensibilisation à la sécurité pour créer et maintenir un comportement positif en matière de sécurité en tant qu'élément essentiel d'un environnement de sécurité de l'information efficace (Kruger et Kearney, 2006).

La formation des employés à la sensibilisation à la sécurité de l'information et à la motivation pour la conformité a un impact positif significatif sur la conformité à la politique de sécurité de l'information (Ma *et al.*, 2009 ; Puhakainen et Siponen, 2010 ; Parsons *et al.*, 2014). La connaissance des politiques et des procédures, acquise par la formation, exerce une influence plus forte sur l'attitude à l'égard des politiques et des procédures que le comportement autodéclaré (Parsons *et al.*, 2014). Afin de maximiser les effets, il est aussi indispensable de recourir à un programme systématique et continu de formation à la sécurité de l'information (Puhakainen et Siponen, 2010). L'étude réalisée par les auteurs confirme que de tels programmes de formation sont un bon moyen d'ouvrir la voie à une communication continue en matière de sécurité de l'information. La sensibilisation, la familiarité et l'expertise des employés sur les questions de sécurité doivent être encouragées et cultivées via des programmes de formation continue et une participation active à des simulations et des exercices de mise en situation modernes (Georgiadou *et al.*, 2022).

⇨ ***Dans le cadre de cette recherche OVSM, le but est de comprendre les pratiques que les dirigeants mettent en œuvre dans le cadre de la gouvernance de la sécurité d'information.***

1.5 L'influence des exigences sociales et environnementales dans la gouvernance de la sécurité de l'information

Les récents progrès des technologies digitales, l'interconnectivité et les outils ont eu plusieurs effets positifs sur les entreprises en termes de rapidité de communication, réduction des coûts, amélioration de l'accessibilité des systèmes ainsi que des effets sur l'efficience et la productivité (Rohan *et al.*, 2023). Les entreprises sont aujourd'hui beaucoup plus flexibles grâce aux solutions technologiques disponibles qui s'adaptent aux changements exigeants et, dans certains cas, violents de l'environnement des affaires (Georgiadou *et al.*, 2022). L'auteur conclut que ce comportement innovant doit également être étendu à la sécurité de l'information, où des écarts radicaux se produisent presque quotidiennement, afin de suivre le rythme du développement et de rester en sécurité à tout moment. En effet, l'hyper-connectivité du paysage actuel de l'information et des médias sociaux fait émerger de nouveaux enjeux relatifs à la génération et la diffusion de fausses informations (Adams *et al.*, 2023) et à la protection des données personnelles à l'heure des mégadonnées (big data) (Hassani, 2019). Le risque numérique peut mettre en péril de manière soudaine et fulgurante les entreprises, ces dernières se doivent de le prendre en compte et de le maîtriser d'autant plus que la responsabilité des dirigeants dans la gestion et le traitement du risque est de plus en plus engagée (Eddé, 2020).

En sus de la technologie, la sécurité de l'information est influencée par un ensemble de facteurs contextuels et environnementaux dont il est indispensable de tenir compte. Les fondements de la sécurité de l'information reposent sur la conscience et la préparation à la sécurité manifestées en toutes circonstances, se transformant et s'adaptant au fil du temps et des changements (Georgiadou *et al.*, 2022). L'étude réalisée par McFadzean *et al.* (2007) démontre que ces facteurs ont trait aux consommateurs, aux partenaires et autres entreprises. En effet, les attentes et les expériences des parties prenantes déterminent le type de programme de sécurité de l'information nécessaire (Lanz et Sussman, 2020).

• La technologie et l'accentuation des nouveaux risques de désinformation

L'innovation technologique dans les domaines de l'intelligence artificielle, du *cloud computing*, de l'analyse des mégadonnées, de la mécanique quantique, de l'Internet des objets, de la *blockchain* et d'autres applications logicielles et matérielles induisent une nécessaire et continuelle évolution de la cybersécurité contemporaine (Wilner, 2018). L'un des risques les plus communément présent avec la transformation numérique des entreprises et des sociétés est celui des *fake news* et de la désinformation (Botha et Pieterese, 2020 ; Petratos, 2021). La désinformation compromet autant les rivaux politiques, les doctrines idéologiques, les relations internationales entre les Etats qu'inter-organisationnelles (Ilieva, 2018). Les progrès technologiques accentuent la

désinformation du fait de l'interconnectivité entre les personnes et l'information et la rapidité avec laquelle la désinformation peut être créée et diffusée à des fins stratégiques (Wilner, 2018).

La désinformation constitue une menace dangereuse pour la sécurité de l'information du 21e siècle (Botha et Pieterese, 2020), car elle peut notamment être utilisée dans le cadre de cyberattaques (Petratos, 2021). La cybersécurité ne consiste pas seulement à protéger les infrastructures ou à protéger les informations, elle implique également de protéger ce que nous savons et la manière dont nous le savons, de sauvegarder l'intégrité des données et de séparer les vérités des faussetés (Wilner, 2018).

• Les collaborateurs et l'exigence de nouvelles formes de travail

Le contexte socioculturel actuel est marqué par un souci d'accroissement du bien-être global et professionnel et favorise ainsi l'acclamation du télétravail (Taskin, 2003). Ce mode de travail, affirme l'auteur, est privilégié pour ses apports en termes de mobilité, de flexibilité et d'autonomie. Il y a aussi un réel engouement chez les jeunes générations qui font du télétravail un critère de sélection des entreprises (Ollivier, 2017). Par ailleurs, le travail à distance a été propulsé par la survenue de la pandémie Covid-19. Les entreprises ont dû déployer de nouvelles technologies dans des délais extrêmement réduits et mettre en place des outils basés sur l'informatique en nuage (cloud computing) pour permettre le télétravail[7] (ou travail à distance) et assurer la continuité des activités[8].

Toutefois, le travail à distance a négativement impacté la cybersécurité et les risques technologiques du fait de l'augmentation des visioconférences qui accentuent la vulnérabilité que les pirates peuvent exploiter (Ahmad, 2020) ou le recours au VPN (Virtual Private Network) qui amplifie la menace pour les individus et les entreprises (Lanz et Sussman, 2020). Les cybermenaces évoluent constamment afin de tirer parti des comportements et des tendances en ligne (Georgiadou *et al.*, 2022). L'étude des auteurs conclue que, dans un contexte de travail à distance, la sécurité de l'information fait partie intégrante des organisations synchrones et se manifeste principalement à travers des solutions technologiques de cybersécurité[9], mais le facteur humain n'est toujours pas reconnu comme un élément central de la chaîne de cybersécurité.

• Les clients et les partenaires et l'application des nouveaux dispositifs juridiques

Les possibilités de connexion gratuite entre les personnes dans le réseau mondial, l'accès à distance aux ressources d'information (y compris les profils personnels), la collaboration au sein de communautés ou l'utilisation de services cloud imposent une nouvelle demande de protection renforcée des données personnelles et du contenu de

[7] *« Désigne l'exercice d'une activité qui s'effectue, en tout ou partie, hors des locaux de l'employeur, grâce aux technologies de l'information et de la communication (internet, téléphonie mobile,* etc.*). » (Ollivier, 2017)*

[8] *Cybersécurité, RSSI et Covid-19 | EY - France*

[9] Des solutions telles que des pares-feux, des logiciels antivirus, des systèmes de détection d'intrusion, des centres d'opérations de sécurité, etc.

l'information (Romansky, 2017). Ainsi, à mesure que l'utilisation des systèmes d'information est devenue omniprésente dans les opérations commerciales et gouvernementales, le nombre de défaillances dans la protection des informations personnelles a augmenté régulièrement (Gillon *et al.,* 2011). Les auteurs confirment que les violations continues des systèmes d'information augmentent les attentes raisonnables des clients quant à la volonté des entreprises de prendre des mesures pour protéger leur sécurité et leur confidentialité. Par ailleurs, À l'heure du *big data,* les données personnelles sont valorisées et constituent un enjeu concurrentiel au cœur de l'économie numérique (Eddé, 2020). Ces données font ainsi l'objet de convoitises à caractère marchand à l'origine de cybercriminalité et de fuites de données massives (Hassani, 2019).

Préoccupés par cette situation, les gouvernements ont établi des réglementations pour le traitement de l'information et la protection des données personnelles (par exemple : le règlement UE 2016/679 sur la protection des données personnelles et sur la libre circulation de ces données (RGPD) entré en vigueur le 25 mai 2018 ; la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) en Suisse). La protection des données personnelles comprend les activités qui doivent garantir les droits des individus si leurs données sont utilisées par des contrôleurs de données et/ou des sous-traitants (Romansky, 2017). Le RGPD recommande des politiques de sécurité de l'information pour toutes les organisations, y compris les Petites et Moyennes Entreprises ainsi que pour les organisations non gouvernementales (Kinnunen, 2017). L'objectif de ces réglementations est de limiter la survenance des risques, minimiser leurs effets s'ils se concrétisent et renforcer les obligations de sécurité et de responsabilisation des entreprises (Eddé, 2020).

- ⇨ ***Dans le cadre de cette recherche OVSM, le focus porte sur la compréhension de l'installation et l'adaptation de pratiques organisationnelles de gouvernance de sécurité de l'information face aux nouvelles exigences sociales et environnementales.***

Chapitre 2
La recherche empirique

Contrairement à la recherche managériale opérationnelle présentée dans la partie I de ce Livre Blanc, la recherche académique utilise des méthodes qualitatives permettant, entre autres, de faire émerger des non-dits et donc d'induire de ceux-ci les dimensions cachées du thème étudié. Bien entendu, ce type de méthodologie mobilise bien plus de temps et de compétences spécifiques de la part des chercheurs que la recherche managériale pour laquelle le facteur temps est primordial.

L'analyse conduite dans le cadre de cette recherche OVSM 2023 est fondée sur la théorie enracinée dans les faits (Ground theory) qui permet le développement d'études et d'analyses sur des sujets d'intérêts sociétaux et économiques majeurs comme c'est le cas pour ce thème de sécurité de l'information. Cette méthodologie est inductive, itérative et comparative. Elle permet également de pouvoir formaliser concepts et théories à partir des données empiriques. Elle se base sur une analyse constante et itérative entre le processus d'analyse et les données du terrain. En outre, cette méthode permet au chercheur de réaliser l'analyse simultanément avec la récolte des données. Ainsi, la conceptualisation et la modélisation évoluent avec l'avancement de la récolte des données, améliorant à chaque étape le modèle final (Bergadaà, 2006).

2.1 La méthodologie de recherche

L'usage d'une méthodologie qualitative permet la compréhension des besoins et des motivations profondes des acteurs (McCraken, 1988). Cette méthodologie a été fréquemment utilisée dans le cadre d'études et recherches sur les phénomènes nouveaux comme ceux de la sécurité de l'information sans cesse remise en cause par les progrès technologiques. Par notre approche subjectiviste, nous nous intéressons au dirigeant et à son appréhension de la sécurité de l'information. Afin d'accéder à cette structure personnelle des individus, nous optons pour des longs entretiens individuels et semi-directifs avec des dirigeants.

Le guide d'entretien comporte 17 questions articulées autour de trois dimensions différentes sur la thématique de la sécurité de l'information (Annexe 1). Les trois thèmes du guide d'entretien sont les suivants : le dirigeant face à ses décisions, la responsabilité des dirigeants dans les mutations organisationnelles et la recherche d'un nouveau contrat sociétal.

Les principaux critères d'échantillonnage dans les recherches qualitatives de type inductif sont d'être représentatifs des théories substantives (liées directement au sujet du décideur en entreprise) et des différences conceptuelles observées lors des travaux exploratoires (liées au thème de la sécurité de l'information). Ont donc été sélectionnés 72 acteurs répondant aux deux critères suivants : (1) membres de la direction (ou ayant une fonction en lien direct avec la direction générale) et de secteurs d'activités variés

(2) exerçant des fonctions leur donnant une perspective propre dans le champ de la sécurité de l'information.

Les interviews d'une durée moyenne de 51 minutes ont été réalisées par des étudiants formés à nos méthodes d'entretien. Toutes les interviews ont été retranscrites. Nous avons opté pour une analyse manuelle de contenu, seule susceptible de nous permettre d'atteindre le « signifié » au-delà du simple « signifiant » énoncé. Nous avons réalisé un portrait individuel de chaque interview. Ces portraits ont tous une structure identique, ils sont organisés selon les principales thématiques de notre objet de recherche. Ces portraits représentent une synthèse, de 4 pages en moyenne, de chaque entretien réalisé.

La saturation des données a été atteinte à la quarante-deuxième retranscription. Ces 42 entretiens sont représentatifs de 8 secteurs économiques (cf. Tableau 2 ci-après).

Tableau 2 – Composition de l'échantillon par secteur et par tranche d'âge

	Nombre d'entretiens	Pourcentage
Banque	4	10%
Biens de consommation	4	10%
Conseil	5	12%
Industrie et construction	5	12%
ONG, Inclusion, Social	4	10%
Santé	3	7%
Services	6	14%
Technologie	5	12%
Autre (transport, luxe)	6	14%
	42	**100%**

	Pourcentage représenté
Moins de 40 ans	5%
Entre 40 et 49 ans	18%
Entre 50 et 59 ans	49%
Plus de 60 ans	28%

2.2 Les résultats et discussion

L'objectif premier de l'analyse du contenu est de dégager la structure générique de chaque acteur (Bergadaà et Nyeck, 1992). Fondée sur l'induction, cette analyse de contenu s'est attelée à comprendre l'organisation sous-jacente aux motivations des dirigeants, les raisons qui fondent leurs comportements et attitudes face à la gouvernance de la sécurité de l'information. Nous présentons, ci-après, le modèle induit de l'analyse de contenu. Ce modèle va être explicité dans les paragraphes qui suivent.

Figure 1 : Modèle induit de l'analyse de contenu

• Les dimensions de la sécurité de l'information

Les entretiens conduisent à deux principales conclusions en matière de dimensions de la sécurité de l'information. La première corrobore les recommandations des chercheurs et a trait à la nécessité de ne pas considérer uniquement la sécurité de l'information selon une vision technique et technologique. Cette dimension n'a jamais été placée en première dimension prioritaire par les dirigeants interviewés. Elle a été soulignée pour attirer l'attention sur le fait que les outils techniques ne doivent pas être négligés et devraient être maîtrisés afin d'éviter la panique en cas d'intrusion. La deuxième conclusion est relative à la multidisciplinarité de la sécurité de l'information.

Par ailleurs, établir une priorité n'est pas une question triviale pour les dirigeants interviewés. Dans certains cas, les dirigeants considèrent la gestion de la sécurité de l'information comme un corollaire de la gestion des risques, les dimensions de l'une deviennent les facettes de l'autre. Dans d'autres cas, le dirigeant considère qu'il ne peut

prioriser une dimension au détriment de l'autre et/ou il trouve que les dimensions de la sécurité de l'information sont toutes interconnectées et liées et doivent de ce fait être simultanément gérées. Par ailleurs, certains dirigeants n'attribuent pas la priorité aux dimensions de la sécurité de l'information, mais à la nature de l'information telle que catégorisée à l'interne (stratégique, confidentielle, publique, interne, etc.) ; ou à l'intégrité de l'information dans le cadre de la prise de décision (sécuriser l'information c'est avant tout s'assurer de son intégrité).

Quand une priorité est établie par le dirigeant, le critère de priorisation est souvent dicté par : le cœur du métier et la nature des activités (pour une compagnie d'aviation, ce sera la dimension humaine et le fait de garantir la sécurité des personnes, pour un conseiller en informatique, la dimension réputationnelle va primer pour une question de compétence) ou par les fonctions exercées au sein de son entreprise (un responsable ressources humaines va placer la dimension humaine en premier tandis qu'un responsable financier aura un intérêt plus particulier pour la dimension financière). Nous présentons, ci-après, l'importance que revêtent les différentes dimensions pour les dirigeants interviewés :

- La **dimension humaine** est fréquemment citée, mais pour différentes raisons. Qu'il s'agisse d'éthique du *business* (mesures légales concernant la protection des données clients ou collaborateur par exemple), ou parce que cette dimension est crainte, car ne pouvant être maîtrisée (le collaborateur est le maillon faible et la cause de dysfonctionnements volontaires ou non), ou parce que la sécurité de l'information est avant tout une responsabilité individuelle (former et sensibiliser) ou pour protéger ses talents (crainte de se faire débaucher un talent par un concurrent).
- La **dimension réputationnelle** prend toute son importance, soit pour les grandes structures qui sont plus visibles (plus on est grand, plus c'est critique), soit pour la nature sensible du métier (banque, conseiller informatique, luxe) soit pour de plus petites structures dont les dommages seraient catastrophiques. A l'ère numérique, une réputation durement acquise peut être très facilement détruite. Ensuite, ces dirigeants arguent du fait que les cyberattaques peuvent arriver, mais ce à quoi il faut veiller c'est d'avoir anticipé et avoir pris toutes les mesures nécessaires afin que cela ne puisse pas fortement impacter la réputation.
- La **dimension stratégique** est primordiale pour des grandes entreprises qui gèrent un très grand nombre de données, car une fuite de données serait d'autant plus catastrophique. Quelques fois, les dirigeants de plus petites structures classent cette dimension en priorité, car la sécurité de l'information est intégrée dans tous les choix stratégiques de leurs entreprises. La sécurité de l'information devient pour les dirigeants une composante à part entière qui doit être développée et inculquée dans la culture organisationnelle.
- La **dimension financière** est essentielle surtout pour les petites structures, car il y a une logique d'investissement à clarifier pour tout ce qui a trait à la sécurité de l'information. Ce qui est intéressant à noter est que quelquefois le risque financier est considéré comme une conséquence des autres risques qui peuvent se matérialiser par une perte de revenus ou perte opérationnelle alors que pour d'autres dirigeants, c'est le volet financier qui donne un cadre à l'action et aux initiatives de protection.

- La **dimension légale** est importante selon la nature du métier (les institutions de droit public par exemple) et au vu des nouvelles législations en matière de protection de données personnelles (en Europe et en Suisse).

  ⇨ ***En réponse à notre interrogation de recherche, le discours des dirigeants conclut que ces derniers perçoivent la sécurité de l'information comme un construit complexe et multi-dimensionnel. Leur défi et focus s'oriente essentiellement vers la cohérence d'action sur ces diverses dimensions interconnectées plutôt que sur l'établissement de priorité d'une(plusieurs) dimension(s) de la sécurité de l'information par rapport aux autres.***

• Le rôle du dirigeant face à la nouvelle donne technologique, sociétale et environnementale

La gouvernance de la sécurité de l'information suppose une vision holistique et pose ainsi le défi au dirigeant de devoir prendre en compte les contextes technologique, sociétal et environnemental. En effet, les entretiens réalisés induisent que la sécurité de l'information doit s'adapter à l'évolution technologique incessante. Cette dernière impacte aussi les interactions de l'entreprise avec ses parties prenantes (collaborateurs, clients et partenaires d'affaires) et la sécurisation des informations entre ces derniers. Les discours des dirigeants interviewés permettent de dresser la posture de la quadripartite (dirigeant, collaborateurs, clients et partenaires d'affaires) en matière de gouvernance de la sécurité de l'information qui est présentée dans les paragraphes qui suivent.

Un contexte technologique marqué par une évolution perpétuelle et une désinformation accentuée

L'ensemble des dirigeants interviewés confirme la tendance naturelle à une rapide et incessante évolution technologique. En matière de sécurité de l'information, les dirigeants soutiennent également que cette tendance (biométrie, calculs quantiques, intelligence artificielle, etc.) serait à la faveur d'un renforcement de la sécurité de l'information et de l'accentuation de ses menaces. Les entretiens rapportent différentes métaphores (les voleurs et les gendarmes, le chat et la souris, le glaive et le bouclier, le miroir à deux faces, etc.) par lesquelles les dirigeants qualifient fréquemment la course sans fin qui se joue entre les systèmes de défense et d'attaques. Malheureusement, ce sont ces dernières qui auraient un pas en avant dans ce système d'ajustement par paliers.

Dans ce contexte d'évolution technologique, les dirigeants affirment que la désinformation reste une menace externe particulièrement problématique (immédiateté de la diffusion et des dégâts) pour la gouvernance de la sécurité de l'information. C'est un phénomène accentué par l'interconnectivité facilitée qu'offrent les réseaux sociaux et la démocratisation des outils de l'intelligence artificielle. L'information est aussi plus facilement acquise, le client, le consommateur et le citoyen sont plus regardants vis-à-vis du comportement des entreprises. Ces dernières, spécifiquement les plus grandes, doivent contrôler tous les niveaux de la chaine d'approvisionnement afin de veiller au

respect des lois, des règles et de l'éthique de leurs entreprises. Il est plus facile de contrôler le premier niveau (signature de contrats et de chartes éthiques), mais dans une société globalisée, l'emprise sur les autres niveaux est plus difficile. A contrario l'impact qui peut toucher l'un des niveaux de la chaîne d'approvisionnement peut se répercuter immédiatement sur l'entreprise.

La désinformation est une problématique sociétale qui dépasse le cadre des affaires. L'information est de plus en plus déstructurée dans son émission et réception et elle est fortement crainte par les dirigeants. Elle peut entacher la confiance qui constitue un fondement essentiel du maintien des relations avec les collaborateurs, les partenaires et les clients. Il ressort également des entretiens que les plus grandes entreprises sont plus touchées par la désinformation que les PME. La taille de ces dernières permet de maintenir des relations personnalisées et régulières avec l'ensemble des parties prenantes et peuvent de ce fait mieux contenir ces phénomènes. La gestion de la désinformation requiert des compétences nouvelles (plus axée sur la communication que la cyber) et certaines entreprises investissent ou font appel à des sociétés externes spécialisées dans l'analyse de signaux faibles sur les réseaux sociaux afin de mieux identifier la désinformation susceptible de constituer un danger pour leur image. Les autres solutions avancées par les dirigeants pour contrer la désinformation ont essentiellement trait à la sensibilisation et au développement d'un esprit critique.

Un contexte environnemental et sociétal favorisant la flexibilité et l'interconnectivité

Des collaborateurs libres et exigeants

Les entretiens soulignent une évolution de l'organisation du travail vers une généralisation et une progression des demandes de temps partiel, d'horaires aménagés ou de télétravail. Ces formes de travail hybride sont réclamées par les nouvelles générations. Elles sont à la recherche de flexibilité et d'un meilleur équilibre vie privée professionnelle, elles sont aussi moins fidèles et plus volatiles dans leurs plans de carrières. Les dirigeants interviewés ne se positionnent pas tous en soutien unanime du travail hybride pour différentes raisons. La sécurité de l'information est l'une de leurs préoccupations, mais elle ne constitue pas la crainte première de cette forme d'organisation. Auparavant, la sécurité focalisait sur le fait d'avoir des outils et technologie impénétrables. Maintenant, ce qui est difficile est de protéger une information qui voyage et qui requiert de sensibiliser et responsabiliser le collaborateur (partage outils professionnels/personnels) ; le coacher sans l'enchaîner (rôle du dirigeant dans l'instauration de la loyauté et la confiance) et de le former à des outils et des technologies adaptées.

La confiance a été souvent positionnée comme condition de la réussite de ces nouvelles formes d'organisation et pour l'atténuation des risques portés à la sécurité de l'information. La technique seule sans communication ne peut créer une relation de confiance avec les collaborateurs. Le risque porté à la sécurité de l'information existe de diluer le rapport qu'il y a entre le collaborateur et l'entreprise. Le collaborateur passe plus de temps dans son environnement privé donc il augmente les risques qu'ils soient

opérationnels ou émotionnels vis-à-vis de de l'entreprise. Au niveau des outils partagés, si le niveau de maturité de l'entreprise en termes de sécurité de l'information est suffisamment élevé, il y a des solutions techniques qui permettent de séparer dans un même outil l'environnement privé de l'environnement professionnel.

Des clients volatiles et alertes et des partenaires interconnectés et sous pression

Les dirigeants interviewés soulignent qu'il y a une attente généralisée de la part des clients concernant la préservation de leurs données personnelles. Pour les entreprises du B2B, cette attente peut donner naissance à des demandes ou des exigences plus poussées (*Non Disclosure Agreement* (NDA) restrictif, certification ISO 27001…). Ces requêtes sont alors discutées au cas par cas. La nature du métier et/ou des activités (médical, militaire, banque, etc.) influent grandement sur la sensibilité que le client peut avoir en matière de sécurisation de l'information. Pour ce qui est des entreprises B2C où les données clients peuvent toucher la sphère privée, la confiance du client est un concept souvent évoqué par les dirigeants. Cette confiance avait par ailleurs été l'un des moteurs du développement du commerce en ligne. A l'inverse des autorités, les clients ne demandent pas de preuve, ils ne requièrent pas spécifiquement cette sécurité de l'information, mais c'est une promesse de vente dont le non-respect peut entraîner des conséquences dramatiques pour l'entreprise. C'est à l'entreprise de faire le premier pas pour garder la confiance du client, l'entreprise doit anticiper pour ne pas décevoir le client.

Les dirigeants ont également pris conscience de l'impact que peut avoir l'interconnectivité des partenaires sur la sécurisation des informations et les contraintes sécuritaires d'un client sont alors transférées à l'entreprise et à l'ensemble des partenaires de la chaine qui doivent adapter leurs processus en conséquence. Toutefois, les dirigeants concernés affirment œuvrer depuis fort longtemps au renforcement de la sécurité de l'information de leurs clients (solutions innovantes, NDA, etc.).

Un dirigeant inspirant et visionnaire

Les entretiens confirment que le dirigeant, au même titre que l'ensemble des autres collaborateurs, est la première personne responsable de la sécurité de l'information qu'il manipule, car c'est une question de déontologie professionnelle. Mais, le rôle du dirigeant est fondamental dans cette responsabilité collective pour laquelle il doit poser le cadre. Les entretiens confirment que le dirigeant se doit d'être exemplaire en la matière pour trois principales raisons. D'une part, sa stature publique accroit sa visibilité et le soumet à une plus large attaque et manipulation de l'information. Il prend ainsi des risques supplémentaires et doit montrer une plus grande vigilance. D'autre part, l'exemplarité du dirigeant est indispensable à cause du très haut degré de sensibilité des informations dont il dispose et des conséquences désastreuses qui peuvent se produire en cas de fuite les concernant. Finalement, l'exemplarité du dirigeant est primordiale, car elle traduit la crédibilité des consignes mises en place et donne une plus forte portée au message. L'attitude et le comportement sont importants,

car les collaborateurs font ce que le dirigeant fait et non ce qu'il dit. De ce fait, l'exemplarité du dirigeant s'est de s'assurer que les comportements traduisent les enjeux stratégiques. Le seul dirigeant a avoir réfuté ce devoir d'exemplarité explicite que la sécurité de l'information est une préoccupation habituelle dans son métier et que les clauses de confidentialité qu'il est amené à signer l'y contraignent ainsi que l'ensemble de ses collaborateurs.

Par ailleurs, le fondement de la sécurité de l'information est la préservation des données de l'entreprise, laquelle a une portée stratégique et devrait naturellement faire partie intégrante et intrinsèque du cahier de charges du dirigeant. Idéalement, il faudrait caractériser le rôle du dirigeant en le définissant mieux, car tout le monde n'en a pas la même compréhension. Toutefois, les entretiens soulèvent la difficulté de cette définition. De plus, le dirigeant n'est pas automatiquement un expert en sécurité de l'information, ce n'est d'ailleurs pas la première compétence évaluée lors de son recrutement. Ainsi, il devrait disposer de compétences minimales lui permettant une prise de conscience, la compréhension des enjeux et l'explicitation de ces derniers à ses collaborateurs. Les personnes interviewées soulèvent qu'il faut aussi éviter de considérer que la sécurité de l'information est un domaine technique relégué à des professionnels. Le dirigeant doit s'y confronter et la discuter de manière approfondie avec ses équipes et montrer que la réussite est un effort collectif qui ne peut être délégué. La sécurité de l'information est aussi un domaine qui évolue rapidement, le dirigeant a l'obligation de se former continuellement afin d'être constamment à jour.

Au-delà des compétences en sécurité de l'information, les entretiens confirment que le rôle premier du dirigeant est d'être un leader inspirant en la matière, de sensibiliser et de s'assurer de la mise en place de toutes les mesures garantissant la sécurité de l'information. Alors que le technicien crée, le rôle du dirigeant est de traduire ces mesures en valeurs, engagement, vision et direction pour ses équipes. Le management est l'élément central de la mise en œuvre de la sécurité de l'information. Alors que la large majorité des interviewés met l'accent sur cet accompagnement, certains le spécifient en parlant de l'importance d'inculquer un esprit critique chez les collaborateurs et rares sont ceux qui insistent sur le volet sanction qui doit accompagner le rôle du dirigeant. Le but ultime évoqué par certains dirigeants est de parvenir à rendre la sécurité de l'information un réflexe dans le comportement quotidien des collaborateurs. Par ailleurs, alors qu'il n'est pas attendu du dirigeant qu'il soit le spécialiste en technologie, il doit toutefois donner la direction à prendre. Le domaine de la sécurité de l'information évolue fortement et très rapidement ce qui requiert du dirigeant d'avoir des compétences minimales lui permettant d'avoir une vision la plus prospective et objective possible dans sa gouvernance de la sécurité de l'information.

⇨ ***En réponse à notre interrogation de recherche, les entretiens réalisés nous permettent d'affirmer que le rôle primordial du dirigeant dans la gouvernance de la sécurité de l'information est fondamentalement lié à l'affirmation de ses qualités de leader visionnaire et inspirant et à la préservation de la confiance des parties prenantes. La confiance est une composante indispensable face à la menace de la désinformation et à l'évolution du contexte sociétal vers une***

plus grande flexibilité du collaborateur et une plus large interconnectivité des acteurs.

• Des pratiques organisationnelles internes axées sur la formation et la sensibilisation pour lutter contre les menaces portées à la sécurité de l'information

La très large majorité des dirigeants, quelque soit leur secteur ou la taille de leur entreprise, ne se considère pas à 100% à l'abri des menaces et des attaques à la sécurité de l'information. Toutefois, certains dirigeants de grandes sociétés soulignent la formalisation de plan de gestion de risques. Ces derniers permettent d'identifier les risques de sécurité d'information en fonction de leur importance et probabilité d'occurrence et clarifient les procédures et mesures en amont qui visent à minimiser l'impact en cas d'incident.

Par ailleurs, la prise de conscience des risques incite les dirigeants interviewés à mettre en place une pléthore de pratiques et d'outils pour anticiper et gérer les risques liés à la sécurité de l'information (*reporting, monitoring, cloud* privé et sécurisé, classification des documents, points d'authentification multiples, sensibilisation, NDA *Non Disclosure Agreement*, anti-virus, certifications ISO, etc.). La systématisation et la sophistication de ces derniers dépendent en premier lieu de la taille de l'entreprise. En effet, l'exposition permanente et quotidienne des grandes structures à des menaces et des cyberattaques les met en état de veille continuel, les conduit à renforcer leurs équipes internes (nomination de DPO-*Data Protection Officer* ou de CISO- *Chief Information Security Officer*, par exemple, ou attribution du rôle de *risk management* de la sécurité de l'information à une personne au sein de chaque équipe) et à investir des budgets conséquents dans les contrats de sous-traitance avec des sociétés externes spécialisées. Mais, dans l'ensemble, l'anticipation et la gestion des risques portés à la sécurité de l'information ont trait à la gouvernance et à la sensibilisation et formation des collaborateurs.

En effet, l'ensemble des dirigeants interviewés s'accordent sur l'importance de la formation et de sensibilisation dans le cadre de la gouvernance de la sécurité de l'information. Les entretiens appuient que l'ère numérique dicte l'importance de la maîtrise des outils sous peine d'être fortement pénalisé. La sensibilisation dépend du domaine d'activité et des caractéristiques personnelles. D'une part, elle est plus simple dans certains secteurs ou l'activité est extrêmement contrôlée et réglementée. Dans ces cas, les dirigeants notent qu'il ne faudrait pas tomber dans l'excès afin de ne pas générer le stress chez les collaborateurs. Sur un plan individuel, la sensibilisation est difficile, car elle est liée à des caractéristiques personnelles et est un subtil mélange d'esprit critique et d'acuité technique.

En matière de formation, plusieurs entretiens ont souligné qu'il est indispensable d'expliciter son importance pour la survie de l'entreprise et l'adapter à chacun et dans un langage simple et compréhensible pour tous. Toutefois, les avis sont partagés sur le ton directif qui doit guider la sensibilisation et la formation. Alors que la majorité évoque un ton directif afin d'implémenter des réflexes et une forte culture sécurité de l'information, plus rares sont ceux qui soulignent que l'arme la plus redoutable est la

confiance qui favorise l'esprit d'initiative et la bonne volonté. La sensibilisation et la formation sont étroitement liées, la réussite de l'une est conditionnée par l'existence de l'autre et plus spécifiquement sa régularité. La frontière entre les deux est aussi difficile à déterminer, certains dirigeants préfèrent ainsi parler de formation pour les techniciens et de sensibilisation pour les autres corps de métier.

Dans la mise en œuvre de la formation, les entretiens conduisent à distinguer essentiellement deux groupes d'entreprises. Celles qui ont formalisé et structuré les programmes de formation et les autres. La formation est une question de budget que les plus grandes structures peuvent débloquer. La majorité de ces dernières disposent de deux types de formations : l'une initiale, évaluée lors du recrutement et l'autre continue, répétée à intervalles réguliers. Les grandes sociétés affirment que la sécurité de l'information amène à ne pas se satisfaire d'un niveau moyen de sécurité de l'information, car celle-ci est définie par le niveau le plus bas dans l'entreprise. Des grandes entreprises disposent aussi souvent d'une équipe sécurité de l'information (différente de l'équipe informatique) qui est spécifiquement chargée de la formation et de la sensibilisation.

Le deuxième groupe d'entreprises est formé de plus petites structures dont la large majorité déplore le manque de moyens financiers permettant la mise en place de formations plus structurées. Les discussions, les présentations et les retours d'expérience sont alors souvent accentués afin de rendre les collaborateurs plus alertes en matière de sécurité de l'information. Pour certaines entreprises, l'absence de formation explicite ou implicite est due à la nature du métier qui, soit présuppose une bonne connaissance de base en la matière (consultant en informatique par exemple), soit n'est pas particulièrement exposé (vendeur en libraire, par exemple). Par ailleurs, dans les deux groupes, les dirigeants soutiennent le recours fréquent à des sociétés externes spécialisées dans le domaine afin de former les collaborateurs et de les tester (faux *phishing*).

Pour ce qui est du contenu des formations, les dirigeants affirment qu'il faut que ces dernières soient axées sur la manipulation des données, mais également sur le comportement et l'attitude à avoir. En matière de type de formations dispensées, il y a une prédominance de la formation en ligne et un plébiscite des cas pratiques et du *testing*. Ces derniers, confirment les dirigeants, produisent un effet plus probant en matière de sécurité de l'information.

- ***En réponse à notre interrogation de recherche, les pratiques que les dirigeants mettent en place pour assurer la gouvernance de la sécurité de l'information varient fortement, dans leur type et degré de formalisation, selon les secteurs d'activité et surtout la taille des entreprises concernées. Toutefois, le point commun à ces pratiques reste l'importance octroyée à la sensibilisation afin de développer des réflexes et une forte culture sécurité de l'information.***

Chapitre 3
Conclusion et perspectives

Cette recherche nous aura permis d'approfondir la connaissance sur la gouvernance de la sécurité de l'information. Nous avons réussi à clarifier le rôle central du dirigeant dans cette gouvernance ainsi que sa perception des dimensions de la sécurité de l'information et des postures de ses principales parties prenantes. Cette étude a induit les facteurs qui influencent l'adoption et la formalisation des pratiques organisationnelles pour répondre aux menaces internes et externes à la sécurité de l'information. D'un point de vue managérial, la recherche OVSM permet de mieux saisir la complexe réalité du dirigeant. Ce dernier est certes « une pièce maîtresse » garant de la sécurisation des données de son entreprise, mais qui doit assurer la cohérence de son action en prenant en considération une multitude de contraintes. Cette étude permet de prendre pleinement conscience que chaque dirigeant devrait participer à son niveau à la consolidation d'un débat de société qui outrepasse les frontières de son entreprise.

Notre recherche qualitative se distingue des traditionnelles recherches quantitatives dans la mesure où elle n'est ni descriptive, ni établissant de simples liens entre des variables d'analyse. D'inspiration structuraliste, notre étude a permis de faire émerger un modèle conceptuel robuste et stable. Certes, le fait d'avoir mené une recherche en Suisse Romande présente une limite relative aux caractéristiques de la situation économique et culturelle de la région, mais pas dans les dimensions du modèle qui, lui, est générique. Il serait intéressant d'étendre l'étude à d'autres régions de Suisse et à d'autres pays pour en comprendre les applications éventuellement différenciées. Nous constatons également une seconde caractéristique dans le fait que notre échantillon comporte une faible proportion de femmes (14%). Or, une récente étude[10] montre que la proportion de femmes à des postes de haute direction est passée de 13% à 20% au cours des toutes dernières années.

L'ère digitalisée a démultiplié les modes d'accès, de diffusion et de traitement de l'information et a de ce fait complexifié sa sécurisation. Cette étude confirme que la technologie qui a facilité l'échange d'information ne constitue paradoxalement pas son bouclier de sécurisation. L'espoir porte essentiellement sur le facteur humain face aux menaces à la sécurité de l'information. C'est au travers d'un effort sociétal collectif, impliquant aussi les acteurs de la formation (primaire à universitaire), que les jeunes, futurs dirigeants de demain, pourront être sensibilisés à cette problématique. Le développement de l'esprit critique est une valeur indispensable à bien des égards et doit être renforcé, car il n'a jamais été autant menacé.

Par ailleurs, l'évolution technologique incessante traduit aussi l'ingéniosité et la curiosité humaines pour construire un monde « meilleur ». Ainsi, les nouvelles

[10] https://www.russellreynolds.com/en/insights/reports-surveys/significant-steps-forward-for-gender-equality-within-swiss-executive-boards?utm_medium=social&utm_source=twitter&utm_campaign=BCAP&utm_content=BCAP%20General

technologies, plus particulièrement l'intelligence artificielle, qui cristallisent les débats ne peuvent absolument pas être occultées par notre monde universitaire. Elles doivent être pensées et étudiées afin de développer un modèle d'enseignement futur garantissant la progression de la connaissance. C'est donc naturellement que la prochaine étude OVSM 2024 portera sur ces questions pour éclairer notre compréhension.

Chapitre 4
Références bibliographiques

Adams, Z., Osman, M., Bechlivanidis, C., & Meder, B. (2023). (Why) is misinformation a problem? *Perspectives on Psychological Science*.

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science*, 72, 361-373.

Ahmad, T. (2020). Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity (April 5, 2020). Available at SSRN: https://ssrn.com/abstract=3568830 or http://dx.doi.org/10.2139/ssrn.3568830

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, 99, 102030.

Al-Harethi, A. A. M., & Al-Amoodi, A. H. A. (2019). Organizational factors affecting information security management practices in private sector organizations. *International journal of psychology and cognitive science*, 5(1), 9-23.

Ambrosi, A., Peugeot, V., et Pimienta, D. (2020). *Enjeux de mots : regards multiculturels sur les sociétés de l'information*. C & F Éditions.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219-238.

Bergadaà, M., & Nyeck, S. (1992). Recherche en marketing : un état des controverses. *Recherche et Applications en Marketing*, 7(3), 23-44.

Bergadaà, M. (2006). Une stratégie de recherche constructiviste appliquée aux services culturels : l'exemple du Musée olympique, de son concept et de ses profils types de visiteurs. *Recherche et Applications en Marketing*, 21(3), 91-113.

Bergadaà, M. (2020). *Le temps entre science et création*. Coll. Les grands auteurs francophones, Éditions EMS, 2020.

Botha, J., & Pieterse, H. (2020). Fake news and deepfakes: A dangerous threat for 21st century information security. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, p. 57.

Chen, C. C., Dawn Medlin, B., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, 16(4), 360-376.

Dagorn, N., & Poussing, N. (2012). Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information. *Systèmes d'information et management*, 17(1), 113-143.

Eddé, R. (2020). Les entreprises à l'épreuve des cyberattaques. *Flux*, (3), 90-101.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35(2), 486-505.

Gillon, K. Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R., & MacWillson, A. (2011). Information Security and Privacy - Rethinking Governance Models. A*ssociation for Information Systems*, Vol. 28, Article 33.

Hashim, R., & Razali, R. (2019). Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model. *International Journal of Innovative Technology and Exploring Engineering*, 9(2), 4491-4499.

Hassani, N. (2019). Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations. Quel cadre éthique offre le RGPD aux data scientists ? Terminal. *Technologie de l'information, culture & société* (124).

Holgate, J.A., Williams, S.P., & Hardy, C.A. (2012). Information Security Governance: Investigating Diversity in Critical Infrastructure. *Proceedings of the 25th Bled eConference 2012, Bled, Slovenia, 20th June 2012*.

Ilieva, D. (2018). Fake news, telecommunications, and information security. *Int. J. Inf. Theor. Appl*, 25(2), 174-181.

ISO-ISO/IEC 27000:2009 - *Information Technology - Security Techniques Information Security Management Systems* - Overview and vocabulary.

Kinnunen, H. (2017). Critical considerations for organisation-specific information security policy development. *International Conference on Transformations and Innovations in Management*, 677-686.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues*, 6(4), 2081- 2094.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25 (4), 289-296.

Lanz, J., & Sussman, B. I. (2020). Information Security Program Management in A COVID-19 World. *The CPA Journal*, 90(6), 28-36.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business*, 30(1).

McCraken, G. (1988). *The long interview*. Newbury Park, Sage

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

Munier, M., Lalanne, V., Ardoy, P. Y., & Ricarde, M. (2014, May). Métadonnées et Aspects Juridiques : Vie Privée vs Sécurité de l'Information. *9e Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information*n, 65-76.

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security, 26(1),* 10-38.

Ollivier, D. (2017). Le succès du télétravail : Les effets de la nouvelle loi Travail. *Études*, 33-46.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, 42, 165-176.

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, 64(6), 763-774.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, Vol. 9, Issue 3, March 2023.

Romansky, R. (2017). A survey of digital world opportunities and challenges for user's privacy. *International Journal on Information Technologies and Security*, 9(4), 97-112.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & security*, 56, 70-82.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? From the basement to the boardroom: towards digital security governance. *Information & Computer Security*, 28(2), 261-292.

Scholl, M. (2018). Information security awareness in public administrations. In *Public Management and Administration,* 27-55.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, 27(5), 644-667.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management*, 36(2), 215-225.

Tan, T., Maynard, S., Ahmad, A., & Ruighaver, T. (2017). Information security governance: a case study of the strategic context of information security. *PACIS 2017 Proceedings*. 43.

Taskin, L. (2003). Les Enjeux du télétravail pour l'organisation. *Reflets et perspectives de la vie économique, XLII*, 81-94.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4), 263-290.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & security*, 23(5), 371-376.

Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal*, 73(2), 308-316.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Zaydi, M., & Nassereddine, B. (2021). A conceptual hybrid approach for information security governance. *International Journal of Mathematics and Computer Science*, 16(1), 47-66.

* *

*

ANNEXES

Annexe 1
Étapes chronologiques de la recherche-interaction de l'OVSM

Étape 1 : Choix du thème annuel et de ses dimensions

Septembre

Le Bureau de l'OVSM détermine le choix du thème annuel, après consultation des membres de l'Association.

Une exposition des photos librement prises ou choisies par les membres comme illustratives du thème donne lieu à un brainstorming. Son résultat permet de concevoir les dimensions du thème de l'année.

Étape 2 : Création et validation du guide d'entretien

Novembre

Le guide d'entretien est affiné et validé par les membres de l'Association OVSM lors d'un repas thématique.

Étape 3 : Sélection des étudiants intervieweurs

Décembre - janvier

Sélection via la Junior Entreprise Genève, d'étudiants-interviewers qui sont formés aux techniques d'entretien par la Dre Fatima Gueroui.

Ces interviewers ont pour rôle de réaliser chacun un ou plusieurs entretiens de hauts dirigeants, avec le support du guide d'entretien.

Étape 4 : Entretiens par les étudiants

Février - Mars

Chacun des étudiants-enquêteurs réalise ses entretiens en face à face avec l'un des dirigeants sélectionnés par l'OVSM.

Étape 5 : Séminaire résidentiel des membres institutionnels – recherche managériale

Mars - Avril

Les représentants des entreprises « Membres institutionnels » de l'OVSM se réunissent pendant deux jours pour discuter du thème de l'année et proposer des pistes d'action.

La synthèse des travaux rassemble les points de vue de l'expert international invité, du sous-groupe « Décisions du dirigeant » et du sous-groupe « Dispositifs organisationnels ».

Présentation à l'Assemblée générale de l'Association OVSM de la synthèse et des recommandations de la recherche managériale opérationnelle.

Étape 6 : Analyse et synthèse des travaux de l'année

Juin - septembre

Analyse qualitative inductive des résultats et proposition du modèle conceptuel. Production du livre blanc annuel.

Étape 7 : Table ronde et débat, événement de clôture

Octobre

Une centaine des dirigeants interrogés sont invités à l'événement de clôture de l'année :

- Présentation de la méthodologie, des résultats, des conclusions et des perspectives de la recherche académique conceptuelle.
- Table ronde
- Débat public

Annexe 2
Le guide d'entretien

Le terme « dirigeant » signifie membre de la direction ayant une fonction en lien direct avec la direction générale et/ou une responsabilité décisionnelle, et ayant des subordonnés.

Le terme « Sécurité de l'information » couvre généralement les données, leur stockage et leur transport, leur valeur et leur intégrité, ainsi que leurs producteurs et utilisateurs (internes et externes). Dans ce guide d'entretien, il couvre aussi les comportements des usurpateurs de ces données et informations.

Thème annuel de recherche-interaction OVSM

Sécurité de l'information - Comment les crises actuelles en clarifient les dimensions

Dimension 1 - individuelle : La décision du dirigeant

[Lire : Les crises qui se sont succédé (pandémie, Ukraine, climat...) ont bousculé les agendas décisionnels de tous les dirigeants. Quel en est l'impact aujourd'hui sur le métier même du dirigeant en entreprise ?]

Q1 Avez-vous déjà été, dans votre activité de dirigeant, confronté à des arbitrages ou débats concernant « la sécurité de l'information » ? Si oui, lequel d'entre eux vous a paru le plus difficile à résoudre ?

> *[aide : c'est au dirigeant, en tant que personne, que l'on s'adresse dans ce thème]*

Q2 Comment classez-vous les priorités des dimensions de la « sécurité de l'information » ?

> *[aide : ex dimensions stratégiques, humaines, financières, opérationnelles, réputationnelles, techniques…]*

Q3 En quoi le comportement du dirigeant doit-il être exemplaire en termes de « sécurisation de l'information » ? Expliquez.

Q4 La sécurisation des informations et des comportements liés appelle-t-elle des programmes de formation ? Si oui, pour qui ?

> *[aide : sécurisation des vidéoconférences, vérification des sources et fake news, exercices d'alerte et de pratique des installations de secours (ex. PC, papier…)]*

Q5 Devrait-on mieux caractériser le rôle du dirigeant pour contribuer à la sécurisation de l'information ? Comment à votre avis ?

[aide : nous entendons par caractéristiques du rôle : réflexes à acquérir, responsabilité plus (ou moins) individualisée, prise de conscience interdisciplinaire, décisions plus rapides …]

Dimension 2 – La responsabilité des dirigeants dans les mutations organisationnelles

[Lire : L'interpénétration des activités, plannings et outils professionnels et personnels lors du COVID-19 ont modifié tant les comportements hiérarchiques que les flux d'information et de données dans les entreprises.

Q6. Les crises se sont accompagnées d'une remise en question des formes d'organisation et d'engagement des collaborateurs. Ces nouvelles formes de travail accroissent-elles les dangers de fuite des informations sensibles ? Si oui, comment et pourquoi ?

[aide : télétravail, désaccord ou démission face à des métiers vidés de leur sens, sabotages, comportements de la hiérarchie obsolètes…]

Q7 Comment sensibiliser le management et les collaborateurs à une culture s'adaptant à ces nouvelles contraintes en matière de sécurisation de l'information sensible ?

[aide : une culture de la sécurité et de la sûreté peut être forte, car intrinsèque au métier (ex. aviation, médecine, armée…) ou faible (contenu non régulé des réseaux sociaux, fraudes par téléphone…)]

Q8 Face aux contraintes et aux risques, quels sont les ressources techniques que le dirigeant peut faire activer ? Sont-elles suffisantes a) au quotidien b) face à une prochaine crise majeure ?

[aide : ordinateurs/ imprimantes/ smartphones mieux sécurisés, centre de données et salle de postes de travail de secours situés à qqs km…]

Q9 Dans votre entreprise, avez-vous des dispositifs pour anticiper et gérer les risques et les différentes alertes internes et externes à la sécurisation des informations quelle que soit leur nature ?

[aide : la très grande majorité des risques informatiques sont internes)

Q10 Les clients de votre entreprise vous demandent-ils de nouveaux comportements en matière de sécurisation et d'utilisation de leurs données personnelles ? Si oui, de quelle nature ?

[aide : suppression des spams publicitaires hyper-profilés reçus avant même la fin d'un achat]

Q11 Quelles conséquences ont les nouveaux dispositifs juridiques (ex. RGPD, échange international des données bancaires avec le fisc, droit à l'image…) face à vos fournisseurs et vos clients, dans votre organisation ?

[aide : simples groupes de réflexion, ou directives strictement appliquées ? Par qui ? Après quelle formation ?]

Dimension 3 : Le contexte socio-économique et international

[Lire : Les perturbations géostratégiques liées aux effets du réchauffement climatique et au refroidissement diplomatique et militaire remettent en cause, entre autres, la logistique et les stratégies internationales. En sont directement impactés : le producteur, le consommateur et le citoyen.

Q12. Comment l'organisation du travail (incluant le rapport « travail/vie privée ») va évoluer et comment cela impacte-t-il la sécurité de l'information ?

> *[aide : smartphone partagé avec l'entreprise, mais parfois volé ou oublié, lieu de coworking aux oreilles indiscrètes…]*

Q13 La société évolue. La désinformation sournoise (greenwashing, information négligente ou trompeuse, fake news en tout genre…) modifie-t-elle la confiance entre employeur/ employé et client/ fournisseur ? Quid de l'avenir ?

> *[aide : le recruteur vérifie-t-il qu'un diplôme n'est pas un faux, que l'e-réputation du candidat est bonne, ou les deux ? Si un client a une image d'activité non « durable », la vérifiez-vous ?*

Q14 Pensez-vous que la technologie évoluera assez rapidement pour faire face aux cyber-attaques (externes) et aux évolutions des comportements individuels malveillants des collaborateurs ou dirigeants (internes) ?

> *[aide : par exemple, via l'intelligence artificielle]*

Q15 Si vous deviez demander aux universités d'adapter leurs enseignements à ce nouvel environnement, quels conseils leur donneriez-vous ?

> *[aide : en termes de structure des programmes, de contenu, de compétences à développer (comme le questionnement et l'esprit critique face à l'information issue du web ou des réseaux sociaux)…]*

Q16 Pour conclure : avez-vous des exemples d'entreprises, en Suisse ou ailleurs dans le monde, qui vous semblent particulièrement actives dans une appréhension de ces diverses mutations ?

Q17 Avez-vous autre chose à ajouter à l'entretien que nous venons d'avoir ?

Source : Copyright OVSM, octobre 2023