Développement d'un outil de diagnostic holistique de la sécurité globale pour les PME : intégration de la sécurité physique, de la cybersécurité et du filtrage de sécurité

par

Francis COATS

MÉMOIRE PRÉSENTÉ À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
COMME EXIGENCE PARTIELLE À L'OBTENTION DU DIPLÔME EN
GESTION DE L'INNOVATION
M. Sc. A.

MONTRÉAL, LE 24 JUILLET 2026

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Michel Rioux, directeur de mémoire
Département de génie des systèmes à l'École de technologie supérieure

M. Marc Paquet, président du jury
Département de génie des systèmes à l'École de technologie supérieure

M. Michaël Gardoni, membre du jury
Département de génie des systèmes à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 25 JUIN 2026

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

AVANT-PROPOS

Au moment de la rédaction de ce mémoire, j'évolue depuis près de vingt-cinq ans dans les domaines de la sécurité physique, de la sécurité de l'information et de la cybersécurité. Au fil de ce parcours, j'ai été amené à collaborer avec plusieurs organismes professionnels reconnus, notamment CANASA et ASIS, ainsi qu'à intervenir régulièrement dans les médias québécois, tels que Radio-Canada, Noovo, le Journal de Montréal, le Journal de Québec et QUB Radio. Mon expertise a notamment été qualifiée comme l'une des plus reconnues en matière de sécurité au Québec (Journal de Québec, 2023).

Je suis titulaire des certifications PSP (Physical Security Professional) et CISSP (Certified Information Systems Security Professional), et j'ai complété, au cours de ma carrière, un grand nombre de formations, d'ateliers et de conférences couvrant l'ensemble du spectre de la sécurité. Cette formation continue, combinée à une pratique soutenue sur le terrain, m'a permis de développer une approche intégrée de la sécurité, fondée à la fois sur des standards reconnus et sur une compréhension concrète des contraintes opérationnelles auxquelles sont confrontées les organisations.

Mon parcours professionnel s'est construit à la fois du point de vue offensif et défensif de la sécurité. En 2003, alors que j'étais policier patrouilleur à la Sûreté du Québec, j'ai intégré une fonction spécialisée en dispositifs de sécurité. Ce rôle consistait à analyser, contourner et neutraliser divers systèmes de protection afin de permettre des interventions discrètes dans le cadre d'enquêtes policières. Cette expérience m'a permis de développer une compréhension approfondie des failles, des vulnérabilités et des limites réelles des dispositifs de sécurité, bien au-delà de leur conception théorique.

À partir de 2007, j'ai orienté ma carrière vers des fonctions de nature défensive et stratégique, notamment comme sergent conseiller en sécurité au sein de la Division de la sécurité gouvernementale et institutionnelle. J'y ai contribué à l'élaboration de politiques de protection, à la conception de stratégies de sécurité physique et à la réalisation d'évaluations de menaces

et de risques pour des institutions de premier plan, incluant des instances gouvernementales et des acteurs internationaux. Parallèlement, j'ai intégré les pratiques de l'informatique judiciaire, ce qui a enrichi mon approche par une meilleure compréhension des enjeux numériques et informationnels.

Toujours à titre de policier, j'ai par la suite agi comme conseiller stratégique en sécurité de l'information auprès du sous-ministre adjoint responsable de la sécurité de l'information gouvernementale et de la cybersécurité au Ministère de la cybersécurité et du numérique du gouvernement du Québec. Cette fonction m'a permis de consolider une vision globale des enjeux de sécurité, à l'intersection des dimensions physiques, humaines et informationnelles. Au cours des vingt-cinq dernières années, j'ai également contribué à la formation de nombreux professionnels de la sécurité au Québec, participant ainsi au développement des compétences au sein de la communauté.

Ce parcours m'a conduit à un constat récurrent : malgré la multiplication des normes, des cadres méthodologiques et des outils d'analyse, l'évaluation de la sécurité demeure souvent incomplète, fragmentée ou insuffisamment rigoureuse. Les audits, analyses de menaces et de risques et évaluations de sites présentent fréquemment des lacunes importantes, en particulier dans l'identification et l'analyse des vulnérabilités résiduelles. Cette situation est encore plus marquée dans les petites et moyennes entreprises, où les ressources et l'expertise sont limitées.

Depuis 2007, j'ai travaillé au développement de plusieurs méthodes et outils visant à améliorer l'analyse et la gestion de la sécurité. L'un de ces outils, qui constitue le cœur de ce mémoire, a été élaboré progressivement sur plus d'une décennie et appliqué de manière empirique dans divers contextes organisationnels. Toutefois, cette approche n'avait jusqu'à présent jamais fait l'objet d'une formalisation scientifique et académique.

Par ce mémoire, je veux structurer et valider cette méthode dans un cadre rigoureux, afin d'en démontrer la pertinence et les limites. Il s'inscrit dans une volonté de contribuer à l'amélioration des pratiques en matière de sécurité globale et d'offrir aux professionnels, mais

surtout au PME et aux particuliers, un outil d'aide à la décision mieux adapté aux réalités contemporaines.

REMERCIEMENTS

Je tiens d'abord à exprimer ma profonde reconnaissance envers mon directeur de recherche, M. Michel Rioux, pour son encadrement rigoureux, sa confiance et ses conseils éclairés tout au long de ce parcours. Son expertise et sa vision ont profondément influencé l'orientation et la qualité de ce mémoire.

Je remercie également l'École de technologie supérieure (ÉTS) pour l'environnement académique stimulant et les ressources mises à ma disposition. Cette maîtrise m'a permis de transformer des années d'expérience terrain et de réflexion en une démarche structurée de recherche et d'innovation.

Mes remerciements vont aussi aux professionnels, collègues et collaborateurs du domaine de la sécurité qui ont accepté d'échanger et de contribuer à cette réflexion. Leur expérience et leur ouverture ont permis d'ancrer cette recherche dans une réalité concrète et opérationnelle.
Je souhaite exprimer une gratitude toute particulière à ma conjointe, Esther. Sans toi, il n'y aurait tout simplement pas eu de mémoire. Merci pour ton soutien inconditionnel, ta patience et ta présence dans les moments les plus exigeants de ce parcours. Derrière chaque page écrite et chaque étape franchie, il y avait aussi ton soutien silencieux, mais indispensable. Ce mémoire porte également une part de toi.

Enfin, je tiens à remercier ceux qui n'ont pas cru en moi, ceux qui confondent image et sécurité réelle, ainsi que ceux qui réduisent la sécurité à un exercice de conformité ou à une simple façade organisationnelle. Je pense également à ceux qui pratiquent une sécurité de complaisance, davantage orientée vers un faux sentiment de sécurité que vers la protection réelle des personnes, des biens et de l'information. Les approches superficielles, les décisions motivées par l'apparence et les mesures implantées pour rassurer plutôt que protéger ont, au fil des années, renforcé ma conviction qu'une sécurité efficace doit être rigoureuse, cohérente et ancrée dans la réalité du terrain. Vous êtes, sans le vouloir, une source constante de motivation.

Développement d'un outil de diagnostic holistique de la sécurité globale pour les PME : intégration de la sécurité physique, de la cybersécurité et du filtrage de sécurité

Francis COATS

RÉSUMÉ

La sécurité dans les petites et moyennes entreprises (PME) est aujourd'hui largement abordée sous l'angle de la cybersécurité, celle-ci étant fréquemment assimilée à la sécurité de l'information dans son ensemble. Or, les menaces cybernétiques ne remplacent pas les menaces traditionnelles touchant les personnes, les infrastructures physiques ou l'information elle-même. Elles s'ajoutent plutôt à un environnement de sécurité déjà complexe. Malgré cette réalité, les différents domaines de la sécurité, notamment la cybersécurité, la sécurité physique et le filtrage de sécurité, demeurent généralement traités de manière indépendante au sein des organisations. Cette approche en silo favorise l'implantation de mesures fragmentées, réactives et parfois incohérentes dans leur déploiement global.

Les cadres normatifs et méthodologies existants sont généralement spécialisés dans un domaine précis de la sécurité et demeurent souvent complexes ou difficilement applicables dans le contexte des PME. De plus, il existe peu d'outils permettant d'évaluer de manière holistique si les mécanismes de sécurité mis en place sont globalement équilibrés et cohérents, tant en fonction des domaines de sécurité que des familles de contrôles et des fonctions opérationnelles des mécanismes de protection.

La présente recherche vise à développer un cadre d'analyse multidimensionnel permettant d'évaluer de manière structurée la posture globale de sécurité des PME à partir d'une approche intégrée et accessible. Contrairement aux approches traditionnelles principalement centrées sur l'analyse de risque ou la conformité réglementaire, la méthode proposée cherche à identifier les déséquilibres organisationnels entre différentes fonctions et composantes de sécurité. Le cadre développé repose sur une matrice structurée selon quatre fonctions de sécurité, soit empêcher, détecter, retarder et répondre, ainsi que trois axes d'intervention : les technologies, équipements et services, les procédures et le facteur humain.

La recherche adopte une démarche qualitative et appliquée reposant sur une revue de littérature, des entrevues réalisées auprès de huit experts reconnus du domaine de la sécurité au Québec, des validations terrain effectuées dans différents contextes organisationnels ainsi qu'un sondage auprès de professionnels de la sécurité. Une analyse exploratoire complémentaire par analyse des correspondances multiples (ACM) et classification ascendante hiérarchique (CAH) a également été réalisée afin d'explorer certaines structures de perception observées chez les répondants.

Les résultats obtenus mettent en évidence plusieurs déséquilibres récurrents dans les pratiques organisationnelles actuelles. Les analyses réalisées suggèrent notamment une forte dominance des approches technologiques, une faible intégration entre les différents domaines de sécurité

ainsi qu'une sous-utilisation des dimensions humaines et procédurales. Les validations effectuées tendent également à démontrer que la représentation visuelle proposée facilite l'identification rapide des forces, faiblesses et asymétries organisationnelles, tout en favorisant les discussions stratégiques entre différents intervenants.

Cette recherche contribue ainsi au développement d'un outil d'analyse structurant, accessible et multidimensionnel visant à soutenir les PME dans l'amélioration progressive de leur posture globale de sécurité à partir d'une approche intégrée adaptée à leurs réalités opérationnelles et à leurs contraintes organisationnelles.

Mots-clés : Sécurité globale, posture de sécurité, PME, cybersécurité, sécurité physique, sécurité de l'information, filtrage de sécurité, gouvernance de la sécurité, analyse de sécurité, gestion de la sécurité, approche holistique, facteur humain, gestion des risques, sécurité organisationnelle, résilience organisationnelle, sécurité multidimensionnelle, visualisation de la sécurité, sécurité des PME, intégration de la sécurité, analyse multidimensionnelle.

Development of a holistic global security diagnostic tool for SMEs: integration of physical security, cybersecurity, and personnel security screening

Francis COATS

ABSTRACT

Security in small and medium-sized enterprises (SMEs) is now largely approached through the lens of cybersecurity, which is frequently assimilated to information security as a whole. However, cyber threats have not replaced traditional threats affecting people, physical infrastructures, or information itself. Rather, they have been added to an already complex security environment. Despite this reality, the different domains of security, notably cybersecurity, physical security, and personnel security screening, continue to be managed independently within organizations. This siloed approach promotes the implementation of fragmented, reactive, and sometimes inconsistent security measures in their overall deployment.

Existing standards and methodologies are generally specialized in a specific security domain and often remain complex or difficult to apply in the context of SMEs. Furthermore, there are few tools capable of holistically evaluating whether implemented security mechanisms are globally balanced and coherent, both in terms of security domains and with respect to the families and operational functions of security controls.

This research aims to develop a multidimensional analytical framework designed to assess the overall security posture of SMEs through an integrated and accessible approach. Unlike traditional approaches primarily focused on risk analysis or regulatory compliance, the proposed method seeks to identify organizational imbalances between different security functions and components. The framework developed is based on a matrix structured around four security functions, namely prevent, detect, delay, and respond, as well as three intervention axes: technologies, equipment and services, procedures, and the human factor.

This research adopts a qualitative and applied methodology based on a literature review, interviews conducted with eight recognized security experts in Quebec, field validations carried out in different organizational contexts, and a survey conducted among security professionals. An exploratory complementary analysis using Multiple Correspondence Analysis (MCA) and Hierarchical Ascending Classification (HAC) was also performed to explore certain perception structures observed among respondents.

The results highlight several recurring imbalances in current organizational security practices. The analyses notably suggest a strong dominance of technological approaches, weak integration between different security domains, and underutilization of human and procedural dimensions. The validations conducted also tend to demonstrate that the proposed visual representation facilitates the rapid identification of organizational strengths, weaknesses, and asymmetries while supporting strategic discussions among stakeholders.

This research therefore contributes to the development of a structured, accessible, and multidimensional analytical tool intended to support SMEs in progressively improving their overall security posture through an integrated approach adapted to their operational realities and organizational constraints.

Keywords: Global security, security posture, SMEs, cybersecurity, physical security, information security, personnel security screening, security governance, security analysis, security management, holistic approach, human factor, risk management, organizational security, organizational resilience, multidimensional security, security visualization, SME security, security integration, multidimensional analysis.

TABLE DES MATIÈRES

Page

LISTE DES TABLEAUX

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ACM	Analyse des correspondances multiples
AICPA	American Institute of Certified Public Accountants
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité
ASD	Adversary Sequence Diagram
ASIS	ASIS International
ASIMM	Association de sécurité de l'information de Montréal
BCP	Plan de continuité des activités
CAH	Classification ascendante hiérarchique
CANASA	Association canadienne de la sécurité
CIIP	Protection des infrastructures d'information critiques
CIMA	Chartered Institute of Management Accountants
CIS	Center for Internet Security
CISO	Responsable de la sécurité de l'information
CISSP	Professionnel certifié en sécurité des systèmes d'information
CMMC	Certification du modèle de maturité de la cybersécurité
COBIT	Control Objectives for Information and Related Technologies
CPTED	Crime Prevention Through Environmental Design
CSF	Cybersecurity Framework
CSO	Chef de la sécurité
CST	Centre de la sécurité des télécommunications

DEA	Défibrillateur externe automatisé
DHS	Department of Homeland Security
DRP	Plan de reprise des activités ou des systèmes
EMR	Évaluation des menaces et des risques
ESRM	Enterprise Security Risk Management
ÉTS	École de technologie supérieure
GRC	Gendarmerie royale du Canada
GTI	Groupe tactique d'intervention
IA	Intelligence artificielle
IAEA	International Atomic Energy Agency
ICIIP	Protection intégrée des infrastructures d'information critiques
ISACA	Information Systems Audit and Control Association
ISED	Innovation, Sciences et Développement économique Canada
ISMS	Systèmes de management de la sécurité de l'information
ISO	Organisation internationale de normalisation
ISO/IEC	Organisation internationale de normalisation / Commission electrotechnique internationale
M Ing	Maîtrise en ingénierie
M Sc A	Maîtrise ès sciences appliquées
MCN	Ministère de la Cybersécurité et du Numérique du Québec
MITRE	The MITRE Corporation
NATO	Organisation du traité de l'Atlantique Nord
NFPA	Association nationale de protection contre les incendies

NIST	Institut national des normes et de la technologie
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting
OIQ	Ordre des ingénieurs du Québec
PCCC	Programme de coordination de la cybersécurité canadienne
PDG	Président-directeur général
PGCD	Plus grand commun diviseur
Ph. D.	Doctorat
PME	Petites et moyennes entreprises
PSP	Professionnel de la sécurité physique
RBQ	Régie du Bâtiment du Québec
SCIAN	Système de classification des industries de l'Amérique du Nord
SOC	System and Organization Controls
SPCA	Société pour la prévention de la cruauté envers les animaux
TI	Technologies de l'information
TRA-1	Méthodologie harmonisée d’évaluation de menace et de risque
TVA	Threat-Vulnerability-Asset
UL	Laboratoires des assureurs
VIP	Very Important Person

INTRODUCTION

Au tournant des années 2020, le monde a été frappé par la pandémie de COVID-19. Face à l'ampleur de la crise, une mobilisation exceptionnelle des ressources humaines, financières et organisationnelles a été mise en place afin de répondre à cette menace sanitaire émergente. Cette priorisation était nécessaire et justifiée. Toutefois, elle n'a pas fait disparaître les autres enjeux de santé publique. Les maladies chroniques, les cancers, les problèmes cardiovasculaires, les troubles de santé mentale et les accidents ont continué d'affecter les populations, parfois avec des conséquences aggravées par la réaffectation massive des ressources vers un seul enjeu dominant.

Cette situation illustre un phénomène bien connu en gestion des risques et des crises : la focalisation intense sur une menace émergente tend à reléguer au second plan des problématiques préexistantes, sans pour autant en réduire la gravité ni la probabilité. Une fois la phase aiguë de la crise passée, les systèmes doivent rééquilibrer leurs priorités afin de retrouver une approche globale et soutenable.

Un phénomène comparable s'observe aujourd'hui dans le domaine de la sécurité organisationnelle. L'émergence et la médiatisation des cybermenaces ont conduit à une concentration croissante des efforts, des budgets et des expertises vers la cybersécurité. Contrairement à la réponse à la pandémie, cette réaffectation des ressources ne s'est toutefois pas inscrite dans une logique temporaire. Elle s'est progressivement institutionnalisée au cours des dernières années, au détriment d'autres domaines fondamentaux de la sécurité.

Les menaces traditionnelles, les vulnérabilités physiques, organisationnelles et humaines, ainsi que les failles liées au filtrage de sécurité des personnes n'ont pourtant pas disparu. Elles demeurent présentes, évoluent et interagissent désormais avec les enjeux technologiques. En concentrant durablement les ressources sur un seul volet de la sécurité, les organisations ont délaissé une grande surface d'attaque plus globale. Paradoxalement, cette spécialisation accrue

s'est accompagnée d'une compréhension partielle et fragmentée des vulnérabilités réelles, malgré des investissements croissants en matière de sécurité.

0.1 Contexte et problématique

Cette section vise à introduire le sujet de recherche en situant le contexte général de la sécurité organisationnelle et en identifiant la problématique à laquelle ce mémoire cherche à répondre. Elle s'articule autour de trois axes : le domaine de recherche, la problématique identifiée et la pertinence du sujet.

0.1.1 Domaine de recherche

La sécurité, au sens large, regroupe l'ensemble des mesures visant à protéger des actifs contre diverses menaces. Un actif peut être défini comme toute ressource, tangible ou intangible, ayant une valeur pour l'accomplissement de la mission d'une organisation et nécessitant une protection. Les actifs tangibles incluent notamment les infrastructures, les bâtiments, les équipements, les personnes et certains supports d'information. Les actifs intangibles comprennent, quant à eux, les données stratégiques, les processus organisationnels, le savoir-faire, la propriété intellectuelle et la réputation de l'organisation (ASIS International, 2023).

La protection de ces actifs mobilise plusieurs domaines d'expertise distincts, notamment la sécurité physique, la sécurité incendie, la protection rapprochée, le filtrage de sécurité, la sécurité de l'information et la cybersécurité. Bien que ces disciplines poursuivent des objectifs communs, elles sont généralement abordées et gérées de manière indépendante. **Cette fragmentation disciplinaire se traduit par des dispositifs de sécurité conçus en silo, où chaque domaine tente de répondre à des menaces spécifiques sans réelle intégration avec les autres volets de la sécurité.**

Dans les grandes organisations, cette fragmentation est parfois compensée par des structures de gouvernance plus formalisées. En revanche, dans les PME, elle conduit souvent à une

absence de vision globale de la sécurité, rendant difficile l'évaluation cohérente de la posture de protection des actifs.

0.1.2 Problématique identifiée

L'une des principales lacunes observées dans la gestion de la sécurité réside dans l'évaluation de la posture de sécurité. Dans le cadre de ce mémoire, la posture de sécurité est définie comme la relation entre la tolérance au risque d'une organisation et les risques résiduels qui subsistent après la mise en place des mesures de sécurité. Une organisation peut être considérée en bonne posture de sécurité lorsque les risques résiduels sont connus, compris et jugés acceptables au regard de sa tolérance au risque.

À l'inverse, une organisation peut se retrouver dans une posture de sécurité inadéquate dans deux situations distinctes. Premièrement, lorsque les risques résiduels dépassent clairement le niveau de risque que l'organisation est prête à accepter. Deuxièmement, lorsque les risques résiduels apparaissent inférieurs à la tolérance au risque uniquement parce qu'ils ont été mal évalués. Cette seconde situation est particulièrement problématique, car elle crée une illusion de sécurité fondée sur une évaluation incomplète ou erronée des risques.

Le risque résiduel constitue la résultante d'une analyse quantitative, qualitative ou hybride de trois variables centrales : les actifs à protéger, les menaces appréhendées et les vulnérabilités résiduelles associées aux mesures ou contrôles de sécurité en place. Bien qu'il existe une multitude de méthodologies permettant d'estimer le risque résiduel, celles-ci seront abordées plus en détail dans les chapitres ultérieurs de ce mémoire. À ce stade, il importe toutefois de retenir que le niveau de risque résiduel dépend directement de la valeur des actifs, de la nature et de l'intensité des menaces, ainsi que du degré de vulnérabilité qui subsiste malgré les mesures de sécurité déployées (voir **Erreur ! Source du renvoi introuvable.**).

Dans de nombreux cas, la mauvaise appréciation des risques résiduels est directement liée à une analyse insuffisante des vulnérabilités résiduelles, qui constituent pourtant une variable

essentielle dans toute évaluation du risque. Lorsque ces vulnérabilités ne sont pas correctement identifiées, documentées et comprises, la posture de sécurité perçue par les décideurs ne reflète pas la réalité opérationnelle du dispositif de protection en place.

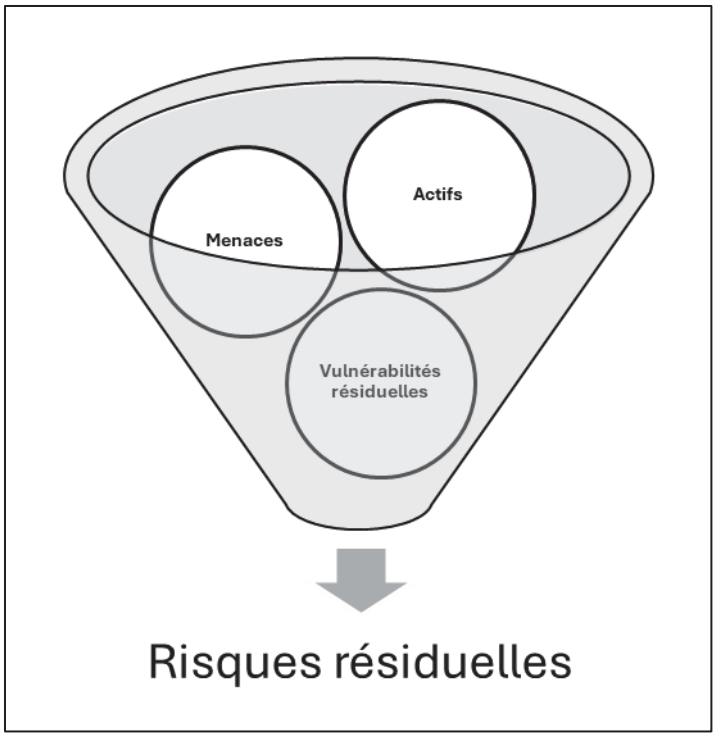


Figure 1.1 Composantes des risques résiduelles

Cette difficulté à évaluer correctement la posture de sécurité s'explique par plusieurs facteurs structurels, qui affectent tant les méthodes d'analyse que l'organisation même de la fonction sécurité.

Premièrement, les évaluations de menaces et de risques sont généralement réalisées de manière cloisonnée par domaine d'expertise. Chaque spécialiste applique ses propres méthodologies, échelles et outils d'évaluation, ce qui génère des résultats hétérogènes et difficilement comparables. Un gestionnaire peut ainsi être confronté à des indicateurs exprimés sous forme de pourcentages, de codes de couleur ou de scores qualitatifs, sans cadre permettant de les

interpréter de manière cohérente. Bien que des tentatives d'harmonisation existent, telles que la Méthodologie Harmonisée d'Évaluation de Menace et de Risque (TRA-1) de la Gendarmerie royale du Canada, celles-ci demeurent peu utilisées et peinent à intégrer l'ensemble du spectre de la sécurité (CST et GRC, 2007). Une autre méthode reconnue de gestion des risques, mais issue d'un domaine différent, mérite d'être mentionnée à ce stade : l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), normalisée notamment par la CEI 60812 (International Electrotechnical Commission). Cette méthode vise à identifier de manière systématique les modes de défaillance potentiels d'un matériel, d'un logiciel ou d'un processus, dont la criticité est généralement estimée à partir d'une combinaison de la probabilité d'occurrence et de la sévérité des conséquences. Cette logique diffère fondamentalement de celle retenue dans ce mémoire, qui ne cherche pas à estimer la probabilité qu'un événement indésirable survienne, mais plutôt à déterminer, dans l'éventualité où il surviendrait, si les mesures de sécurité en place permettraient d'y faire face adéquatement. Pour cette raison, l'AMDEC est écartée comme méthode comparable dans le cadre de cette recherche.

Deuxièmement, les analyses de sécurité mettent fréquemment l'accent sur les menaces et la valeur des actifs, au détriment de l'analyse des vulnérabilités. Or, la vulnérabilité constitue un élément central dans toute évaluation du risque. Son omission, qu'elle résulte d'une méconnaissance, d'un manque d'expertise ou d'une complaisance organisationnelle, laisse subsister des failles critiques non traitées. Ces vulnérabilités sont souvent d'ordre humain, procédural ou organisationnel, et demeurent difficiles à identifier sans une approche structurée et globale.

Troisièmement, les organisations présentent fréquemment des déséquilibres marqués dans l'application des mesures de sécurité. Ces déséquilibres se manifestent tant dans les types de mesures déployées que dans la couverture des fonctions de sécurité. L'accent est majoritairement mis sur les équipements et les technologies, alors que les procédures et la formation du personnel sont négligées. De plus, les investissements visent principalement à empêcher ou détecter les menaces, sans garantir des capacités suffisantes pour retarder ou

répondre efficacement à un incident. Ces déséquilibres affaiblissent la posture de sécurité globale, même lorsque des analyses de risques formelles ont été réalisées.

Enfin, la gouvernance de la sécurité constitue un facteur aggravant. Dans de nombreuses organisations, et plus particulièrement dans les PME, les rôles et responsabilités en matière de sécurité sont rarement clairement définis voir même inexistants. Quand ils existent, ils sont dispersés entre plusieurs départements. L'absence d'une autorité centralisée, telle qu'un chef exécutif de la sécurité (Chief Security Officer) chapeautant l'ensemble des volets de la sécurité, complique la coordination et la cohérence des décisions. Cette fragmentation hiérarchique renforce la dichotomie entre les approches physiques, informationnelles et humaines, alors que les risques résiduels devraient être évalués de manière intégrée.

0.1.3 Pertinence du sujet de recherche

Le besoin d'améliorer l'évaluation et la gestion de la sécurité est d'autant plus critique que les coûts associés aux mesures de protection augmentent, tout comme les impacts potentiels des incidents de sécurité. Qu'il s'agisse de menaces intentionnelles ou d'événements accidentels, les conséquences peuvent compromettre durablement la pérennité d'une organisation.

Le contexte géopolitique actuel accentue ces enjeux. La montée des tensions économiques, la banalisation des techniques d'espionnage industriel et la facilité d'accès à des moyens d'attaque sophistiqués exposent davantage les PME, qui disposent rarement des ressources nécessaires pour évaluer correctement leur posture de sécurité globale. Dans ce contexte, le développement d'outils simples, accessibles et intégrés devient un levier essentiel pour améliorer la résilience organisationnelle.

0.2 Objectif du mémoire

L'objectif principal de ce mémoire est de développer un outil d'analyse et de diagnostic de la sécurité globale axé sur les vulnérabilités résiduelles destiné aux petites et moyennes entreprises. Ce développement s'appuie sur la présomption qu'il n'existe pas, à ce jour, d'outil

simple, accessible et réellement holistique permettant d'évaluer de manière intégrée l'ensemble du spectre de la sécurité dans le contexte des PME, présomption qui sera examinée et validée dans le cadre de la revue de littérature.

Le mémoire vise, dans un premier temps, à analyser les approches, cadres et outils actuellement utilisés pour l'évaluation de la sécurité afin d'en identifier les limites lorsqu'ils sont appliqués à une perspective globale. Cette analyse permet d'évaluer dans quelle mesure les méthodologies existantes couvrent de façon cohérente les différents domaines de la sécurité, notamment la sécurité physique, la sécurité de l'information, la cybersécurité et le filtrage de sécurité des personnes, tout en tenant compte des contraintes propres aux PME.

Sur la base de cette analyse, **le mémoire propose le développement d'un outil de diagnostic conçu pour être volontairement simple d'utilisation, afin de contribuer à la démocratisation de l'analyse de la sécurité**. L'outil vise à permettre à un utilisateur, qu'il soit gestionnaire ou responsable non spécialiste, d'identifier où se situent les vulnérabilités de son organisation en matière de sécurité globale, et ainsi de mieux orienter les problématiques vers les professionnels et expertises appropriés.

L'outil développé a également pour objectif d'évaluer l'approche holistique de la sécurité en considérant simultanément plusieurs domaines de la sécurité et en analysant l'homogénéité des mesures de protection mises en place. Cette évaluation repose sur deux dimensions complémentaires : d'une part, la couverture des fonctions fondamentales de sécurité, et d'autre part, la répartition des contrôles selon les axes d'intervention (familles) que sont les technologies, les équipements et les services, les procédures et le facteur humain. En mettant en évidence les déséquilibres et les lacunes dans ces dimensions, l'outil vise à offrir un portrait clair, structuré et exploitable de la posture de sécurité globale d'une organisation.

0.3 Structure du document

Ce mémoire est structuré en six chapitres, suivant une progression logique allant des fondements théoriques vers l'analyse empirique, la conception de l'outil et l'interprétation des résultats obtenus.

Le premier chapitre présente une revue de la littérature portant sur les concepts fondamentaux liés à la sécurité, à la sécurité de l'information, à la cybersécurité, au filtrage de sécurité ainsi qu'aux approches d'analyse des vulnérabilités et de gestion des risques. Ce chapitre vise à établir les bases conceptuelles du mémoire, à clarifier la terminologie utilisée et à identifier les limites des approches actuellement proposées dans la littérature scientifique et professionnelle, particulièrement dans le contexte des petites et moyennes entreprises.

Le deuxième chapitre présente une synthèse d'entrevues réalisées auprès d'experts reconnus issus de différents domaines de la sécurité. Ces praticiens apportent une perspective opérationnelle complémentaire à la littérature académique. Ce chapitre permet notamment de documenter les réalités terrain observées dans les organisations, les principaux enjeux de gouvernance de la sécurité ainsi que les limites pratiques des approches actuellement utilisées.

Le troisième chapitre décrit la méthodologie de recherche retenue dans le cadre de ce mémoire. Il présente l'approche méthodologique utilisée, les choix de recherche effectués, les méthodes de collecte et d'analyse des données ainsi que le processus général ayant guidé le développement de l'outil proposé.

Le quatrième chapitre présente la conception de l'outil d'analyse de la posture de sécurité globale développé dans le cadre de cette recherche. Il décrit les principes structurants du modèle, les dimensions d'analyse retenues, la logique de catégorisation des contrôles ainsi que la représentation visuelle permettant d'illustrer les forces et faiblesses d'une posture de sécurité.

Le cinquième chapitre présente la validation empirique de l'outil ainsi que l'analyse des résultats obtenus lors de son application en contexte réel. Il expose les observations recueillies, les réactions des participants, les tendances observées ainsi que les principaux constats découlant des validations réalisées auprès de professionnels et d'organisations.

Le sixième chapitre propose une discussion et une analyse des résultats obtenus. Il met en lumière les contributions théoriques et pratiques du modèle développé, les limites observées, les enjeux d'application ainsi que les perspectives d'amélioration et d'évolution futures de l'outil proposé.

Enfin, la conclusion synthétise les principales contributions du mémoire, rappelle les éléments centraux démontrés dans le cadre de cette recherche et présente certaines pistes de recherche futures.

CHAPITRE 1

REVUE DE LITTÉRATURE

La sécurité organisationnelle est aujourd'hui abordée à travers une multitude de disciplines, de cadres normatifs et de méthodologies spécialisées. Cette diversité témoigne de la richesse du champ, mais elle contribue également à une fragmentation des connaissances et des pratiques, rendant difficile l'évaluation cohérente de la posture de sécurité globale d'une organisation, en particulier dans le contexte des petites et moyennes entreprises.

Dans ce contexte, ce chapitre vise à établir les fondements théoriques, scientifiques et documentaires sur lesquels s'appuie la recherche présentée dans ce mémoire. Il repose exclusivement sur une revue de la littérature issue de sources académiques, normatives et institutionnelles reconnues. L'objectif est de clarifier les concepts fondamentaux de la sécurité, d'examiner les cadres existants se voulant holistiques ou spécialisés par domaine, et d'identifier les limites documentées de ces approches en matière d'évaluation de la posture de sécurité globale.

Le chapitre est structuré en quatre sections principales. La première section est consacrée à la clarification de la terminologie, des concepts et du périmètre de la sécurité organisationnelle. La deuxième section examine les cadres et approches se voulant holistiques en matière de sécurité. La troisième section analyse les cadres, normes et méthodologies développés par domaine d'expertise. Enfin, la quatrième section met en évidence le rôle central des vulnérabilités dans l'évaluation de la posture de sécurité et synthétise les principales lacunes identifiées dans la littérature.

1.1 Terminologie, concepts et périmètre de la sécurité

Avant d'aborder les cadres méthodologiques et les approches analytiques en matière de sécurité organisationnelle, il est essentiel d'établir une compréhension commune des concepts fondamentaux mobilisés dans ce mémoire. La littérature scientifique et normative démontre

que plusieurs notions liées à la sécurité sont fréquemment utilisées de manière imprécise ou interchangeable, ce qui contribue à des confusions conceptuelles et, par conséquent, à des dispositifs de sécurité incomplets ou déséquilibrés.

Dans le contexte de cette recherche, la clarification terminologique revêt une importance particulière, puisque les sections subséquentes abordent différents volets de la sécurité de l'information, de la sécurité physique et du facteur humain. Sans un cadre conceptuel clair et partagé, l'analyse des cadres existants et l'évaluation de leur portée holistique risqueraient de reposer sur des prémisses ambiguës.

Cette section vise donc à définir et à contextualiser les principaux concepts nécessaires à l'analyse de la sécurité globale. Elle débute par un bref rappel historique permettant de situer l'émergence et l'évolution de la sécurité de l'information. Elle présente ensuite le contexte organisationnel des petites et moyennes entreprises, précise la notion d'actif et les enjeux liés à sa protection, puis aborde successivement les principaux domaines de la sécurité, soit la sécurité physique, le filtrage de sécurité des personnes, ainsi que la sécurité de l'information et la cybersécurité.

1.1.1 Bref historique de la sécurité de l'information et clarification conceptuelle

Bien que ce mémoire porte plus largement sur les enjeux de sécurité globale au sein des organisations, il demeure essentiel d'aborder le concept de sécurité de l'information, puisque celui-ci occupe aujourd'hui une place importante dans les PME, les médias, les discours gouvernementaux ainsi que dans les pratiques organisationnelles. Pourtant, ce terme est souvent utilisé de manière imprécise, ambiguë ou réduit à tort à la seule cybersécurité. Cette confusion conceptuelle influence directement la manière dont les organisations perçoivent les menaces, structurent leurs mesures de protection et répartissent leurs ressources en sécurité.

Dans la littérature contemporaine, la sécurité de l'information est fréquemment assimilée à la cybersécurité. Cette assimilation est observable tant dans les discours organisationnels que

dans les pratiques professionnelles, médiatiques et institutionnelles. Pourtant, sur le plan théorique et normatif, une distinction claire peut être établie entre ces deux concepts. La sécurité de l'information vise la protection de l'information indépendamment de sa forme ou de son support, alors que la cybersécurité se concentre plus spécifiquement sur la protection des systèmes numériques, des réseaux et des technologies de l'information (ISO/IEC, 2022a ; Alexei et Alexei, 2023 ; Von Solms et Van Niekerk, 2013 ; Taherdoost, 2022 ; Pittala et Ashok, 2023).

Bien que cette distinction soit clairement établie dans les cadres conceptuels et normatifs, elle tend toutefois à s'estomper dans la pratique. Les termes « sécurité de l'information » et « cybersécurité » sont fréquemment utilisés de manière interchangeable dans la littérature académique, les documents de politiques publiques et les discours organisationnels. Plusieurs travaux soulignent que cette confusion terminologique contribue à une compréhension partielle, voire réductrice, du périmètre réel de la sécurité de l'information, en la ramenant essentiellement à des enjeux numériques ou technologiques, tout en marginalisant les dimensions humaines, physiques et organisationnelles. Bien que la cybersécurité soit un sous domaine de la sécurité de l'information, c'est le contraire qu'on voit fréquemment dans les entreprises et les organisations. Même venant d'organisme comme ISO. Le simple titre de la norme ISO 27002:2022 à savoir « Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information » semble exclure d'emblée plusieurs autres sous-domaines de la sécurité de l'information comme la sécurité physique ou le filtrage de sécurité des employés. Cette situation n'est guère étonnante quand on lit au début de la norme : « Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, Technologies de l'information, sous-comité SC 27, Sécurité de l'information, cybersécurité et protection de la vie privée. » (ISO/IEC, 2022a). Donc le comité chargé de rédiger cette norme sur la sécurité de l'information relève dans les faits (c'est un sous-comité) du comité Technologies de l'information.

Cette réduction conceptuelle se reflète également dans les structures organisationnelles et dans la littérature empirique portant sur la gouvernance de la sécurité. Plusieurs études empiriques

analysant le rôle du Chief Information Security Officer montrent que, dans de nombreuses organisations, ce rôle est principalement centré sur la sécurité des technologies de l'information et la cybersécurité. Ces travaux documentent des responsabilités associées aux systèmes informatiques, aux réseaux, à la protection des données et à la gestion des risques numériques, sans aborder les dimensions relatives à la sécurité physique, à la sécurité du personnel ou à la sécurité organisationnelle globale. Cette focalisation contribue à renforcer, dans la pratique, l'assimilation de la sécurité de l'information à la seule cybersécurité (Da Silva et Jensen, 2022 ; Karanja et Rosso, 2017).

Afin de clarifier cette assimilation réductrice, il apparaît pertinent de revenir aux fondements mêmes du concept de sécurité de l'information. Une analyse historique permet de replacer ce concept dans une perspective plus large que celle, relativement récente, des technologies numériques. Comprendre la sécurité de l'information implique d'abord de comprendre ce qu'est l'information, les formes qu'elle a prises au fil du temps et les enjeux de protection qui en ont découlé.

L'information peut être définie, au sens large, comme un contenu structuré permettant de transmettre un sens, une connaissance ou une instruction. Sur le plan étymologique, le terme « information » provient du latin informatio, dérivé du verbe informare, signifiant « donner une forme », « façonner », « former l'esprit » ou encore « instruire » (Etymonline, s.d.). Le terme information renvoie ainsi avant tout à un processus de mise en forme du sens destiné à être compris par un destinataire, et non à un support technique particulier.

Bien avant l'apparition des technologies de l'information, l'information existait déjà sous forme orale. L'émergence du langage verbal a constitué la première forme d'information organisée, permettant la transmission de savoirs, de règles sociales, de croyances et de connaissances acquises empiriquement. Bien qu'il soit difficile de dater précisément cette émergence, car le langage ne laisse pas de traces fossiles directes, on situe à environ 50 000 à 100 000 ans le langage moderne à savoir la syntaxe et la combinaison hiérarchique des mots

(Nowak et Krakauer, 1999). Dans ce contexte pré technologique, la disponibilité de l'information était vitale.

Néanmoins, les premiers mécanismes de sécurité de l'information reposaient ainsi sur des formes d'habilitation implicites, fondées sur la confiance, l'appartenance au groupe, au clan ou à la communauté. L'accès à certaines connaissances (caractéristique de confidentialité de l'information) était réservé aux membres reconnus du groupe, tandis que les individus extérieurs en étaient exclus. La littérature anthropologique et sociologique montre que ces mécanismes de filtrage informationnel, basés sur la confiance sociale et l'identité collective, constituaient le principal moyen de protection de l'information dans les sociétés pré technologiques (Bowles et Gintis, 2004 ; Erickson, 1981 ; DeConick, 2022 ; Bingley, Greenaway et Haslam, 2022)

Plus tard, l'apparition de l'écriture a marqué une transformation majeure dans l'histoire de la sécurité de l'information, en permettant la fixation et la transmission de l'information sur des supports matériels durables. Toutefois, bien avant l'émergence de systèmes d'écriture formalisés, les sociétés humaines avaient déjà développé des formes avancées de communication symbolique. Les peintures rupestres constituent l'un des premiers exemples documentés de représentation graphique de l'information. Des œuvres pariétales telles que celles de la grotte Chauvet, datées d'environ 30 000 ans, témoignent d'une capacité de transmission du sens au sein des groupes humains (Valladas *et al.*, 2001). Des découvertes encore plus anciennes en Indonésie, notamment à Sulawesi, montrent des scènes de chasse datées d'au moins 43 900 ans, considérées comme les plus anciennes formes connues de narration figurative et d'art symbolique (Aubert *et al.*, 2019).

Contrairement au langage oral, qui repose sur une communication synchrone nécessitant la présence simultanée de l'émetteur et du récepteur, la représentation symbolique et, plus tard, l'écriture ont introduit une transformation majeure des modalités de transmission de l'information. Les travaux en anthropologie et en linguistique décrivent l'écriture comme un système symbolique permettant l'objectivation du langage, c'est-à-dire sa mise en forme sous

une forme stable pouvant être conservée, distribuée et consultée dans des contextes distincts de celui de sa production (Chen, 2016). Cette objectivation permet au message d'être détaché du contexte immédiat de son énonciation, en rompant avec les contraintes interactionnelles propres au langage oral, lequel requiert une interaction synchrone pour assurer la transmission du sens.

Par ailleurs, la littérature portant sur les systèmes symboliques montre que ces formes de représentation permettent une séparation temporelle et spatiale entre la production et l'interprétation de l'information. En dissociant l'acte de création du message de celui de sa réception, l'écriture et la représentation symbolique rendent possible une circulation de l'information indépendante de la présence simultanée des acteurs de la communication (Guasch *et al.*, 2013). Sur la base de ces apports, il est possible d'analyser l'écriture comme une technologie de communication rendant possibles des interactions asynchrones, en contraste avec le caractère intrinsèquement synchrone du langage oral.

Cette évolution a entraîné l'émergence de nouveaux enjeux de sécurité de l'information. Alors que le langage oral reposait principalement sur le contrôle social, la confiance et l'appartenance au groupe pour réguler l'accès à l'information, la fixation de l'information sur des supports matériels a introduit des problématiques inédites liées à la protection physique des supports, à la conservation dans le temps et à la gestion de l'accès à des informations dissociées de leur auteur. L'écriture n'a donc pas créé l'information, mais a transformé en profondeur ses modes de transmission et, par conséquent, les mécanismes nécessaires à sa sécurisation.

L'avènement des technologies de l'information et de l'information numérique a profondément modifié les caractéristiques de l'information, notamment en augmentant la vitesse de diffusion, la portée géographique et la facilité de reproduction, des transformations largement documentées dans la littérature théorique sur l'information numérique (Tsvetkov, 2024). Cette transformation a donné naissance à des risques spécifiques liés aux systèmes informatiques et aux réseaux, menant à l'émergence de la cybersécurité comme domaine spécialisé. Toutefois,

cette spécialisation ne saurait faire disparaître les autres formes d'information ni les mécanismes de protection qui leur sont associés.

Après avoir défini ce qu'est l'information, il convient maintenant de préciser la notion de sécurité. Sur le plan étymologique, le terme « sécurité » provient du latin *securitas*, dérivé de *securus* (se- et *cura*), signifiant « exempt de souci », « sans inquiétude » ou « à l'abri du danger » (Etymonline, [s d]). Cette origine met en évidence que la sécurité renvoie, à un état recherché de protection et de tranquillité, avant toute formalisation technique, organisationnelle ou normative. La sécurité ne désigne donc pas, à l'origine, un ensemble de moyens ou de dispositifs, mais un état recherché visant à limiter l'exposition à l'incertitude et aux événements indésirables.

Ces perspectives historiques et sémantiques mettent en évidence que la sécurité de l'information ne se limite pas à la protection de l'information numérique. Comme le rappelle le National Institute of Standards and Technology dans sa publication SP 800-12, elle englobe bien la protection de l'information sous toutes ses formes, qu'elle soit verbale, physique ou numérique (Nieles, Dempsey et Pillitteri, 2017). Assimiler la sécurité de l'information à la seule cybersécurité revient ainsi à réduire artificiellement son périmètre et à laisser subsister des surfaces d'attaque pourtant bien documentées dans la littérature scientifique. Ce constat justifie la nécessité d'une approche plus large et intégrée de la sécurité de l'information, qui constitue l'un des fondements conceptuels de ce mémoire.

1.1.2 Les petites et moyennes entreprises au Canada

La définition des petites et moyennes entreprises constitue un préalable essentiel à cette recherche, puisque l'outil d'analyse développé dans ce mémoire vise spécifiquement ce type d'organisation. Selon Innovation, Sciences et Développement économique Canada (ISED), une petite entreprise compte de 1 à 99 employés rémunérés, tandis qu'une moyenne entreprise regroupe de 100 à 499 employés rémunérés. Une PME est ainsi définie comme une entreprise

comptant entre 1 et 499 employés rémunérés (Innovation, Sciences et Développement économique Canada, 2025).

Au-delà de cette définition quantitative, les PME occupent une place centrale dans l'économie. Au Canada, dans les dernières années, elles représentent plus de 99 % des entreprises actives et constituent le principal moteur de création d'emplois, regroupant plus de 60% de la main-d'œuvre du secteur privé. Leur contribution économique est également majeure, les PME générant environ la moitié du produit intérieur brut du secteur privé en 2021 (Innovation, Sciences et Développement économique Canada, 2025). Cette réalité se retrouve de manière comparable dans la majorité des économies industrialisées, où les PME jouent un rôle structurant dans la vitalité économique, l'innovation et la résilience des chaînes d'approvisionnement.

Les petites et moyennes entreprises (PME) jouent un rôle stratégique important dans les économies nationales; toutefois, elles présentent des caractéristiques organisationnelles distinctes qui influencent directement leur posture globale de sécurité. Aux États-Unis et au Canada, les PME disposent généralement de ressources financières, humaines et techniques plus limitées que les grandes organisations. Elles ont souvent un accès restreint au capital et aux ressources financières, ce qui affecte leur capacité à investir dans l'innovation et les initiatives de croissance (Chen, 2024). De plus, les PME s'appuient habituellement sur des effectifs plus réduits et disposent de moins de talents spécialisés que les grandes entreprises, ce qui peut limiter leur capacité dans des fonctions organisationnelles critiques telles que la recherche et développement, le marketing et d'autres domaines opérationnels (Ogunyomi et Bruning, 2016).

Cette configuration structurelle se traduit fréquemment par une concentration des responsabilités de gestion, d'opérations et, le cas échéant, de sécurité entre les mains d'un nombre restreint d'individus, parfois même d'un seul dirigeant. Si cette concentration peut favoriser une approche pragmatique et opérationnelle de la gestion de la sécurité, elle peut

également restreindre la capacité de l'organisation à développer des programmes structurés et spécialisés couvrant l'ensemble des domaines de la sécurité organisationnelle.

La littérature souligne que cette contrainte structurelle expose les PME à des vulnérabilités spécifiques. En matière de cybersécurité, les PME sont régulièrement ciblées par des attaques opportunistes, notamment en raison d'un manque de ressources spécialisées, d'une maturité limitée des pratiques de sécurité et d'une expertise interne souvent insuffisante (Ambreen *et al.*, 2024). Toutefois, les enjeux de sécurité ne se limitent pas au domaine numérique. Les petites et moyennes entreprises demeurent également vulnérables à des incidents de sécurité physique, à des actes d'espionnage économique, à des vols d'information ainsi qu'à des menaces liées au facteur humain, telles que la négligence, l'ingénierie sociale ou la compromission interne (Coles-Kemp, 2009 ; Von Solms et Van Niekerk, 2013 ; ISO/IEC, 2022a).

Plusieurs études indiquent que les atteintes à la sécurité au sein des PME peuvent entraîner des conséquences disproportionnées par rapport à leur taille, notamment en raison de ressources financières, humaines et organisationnelles plus limitées. Une interruption d'activité, une perte d'information sensible ou un incident affectant la confiance des clients peut menacer directement leur survie (Manish Keshavrao Hadap *et al.*, 2025). Contrairement aux grandes organisations, les PME disposent rarement de capacités de redondance ou de plans de continuité pleinement formalisés, ce qui accentue l'impact des incidents de sécurité (De Matteis, Elia et Del Vecchio, 2023).

Ces constats mettent en évidence un paradoxe fondamental. Bien que les PME constituent un pilier économique essentiel, leur sécurité demeure souvent fragmentée, réactive et orientée vers des enjeux immédiats. Cette situation justifie la nécessité de disposer d'outils d'analyse de la posture de sécurité adaptés à leur réalité organisationnelle, permettant d'évaluer de manière globale, cohérente et accessible les forces et les vulnérabilités des dispositifs de sécurité en place. C'est précisément dans cette perspective que s'inscrit la démarche proposée dans ce mémoire.

1.1.3 Base de la sécurité en entreprise

Indépendamment de la sphère de sécurité considérée, la sécurité organisationnelle est fondamentalement orientée vers le soutien de la mission de l'organisation. Les fonctions de sécurité sont conçues pour protéger les actifs critiques et pour limiter les perturbations, les pertes et les impacts susceptibles de compromettre l'atteinte des objectifs stratégiques et opérationnels ainsi que la continuité des activités (ASIS International, 2021 ; ISO/IEC, 2019 ; ISO/IEC, 2018).

Pour atteindre cet objectif, la sécurité organisationnelle repose sur la protection des actifs de l'entreprise. Ces actifs peuvent être tangibles, tels que les personnes, les bâtiments, les équipements ou les infrastructures, ou intangibles, comme l'information, la propriété intellectuelle, la réputation ou les processus organisationnels. La compromission d'un actif, quelle que soit sa nature, peut nuire directement à la capacité de l'organisation à remplir sa mission (ASIS International, 2021),

La protection des actifs s'appuie traditionnellement sur des démarches d'analyse du risque. Bien que plusieurs méthodes et cadres existent, et seront examinés plus loin dans ce mémoire, il est possible d'en dégager une logique commune. Le risque est généralement appréhendé comme une résultante, qualitative ou quantitative, de plusieurs variables interdépendantes, notamment les actifs, les menaces et les vulnérabilités (ASIS International, 2021 ; NIST - Joint Task Force Transformation Initiative, 2012).

Les menaces peuvent être de nature intentionnelle ou non intentionnelle. Les menaces intentionnelles, parfois qualifiées de menaces « pensantes », incluent par exemple l'espionnage, le sabotage, la fraude ou les actes malveillants visant délibérément les actifs de l'organisation. Les menaces non intentionnelles, dites « non pensantes », regroupent notamment les défaillances techniques, les erreurs humaines, les incidents opérationnels ou les événements environnementaux (NIST - Joint Task Force Transformation Initiative, 2012 ;

ASIS International, 2021). Dans tous les cas, une menace ne peut avoir d'impact que si elle exploite une vulnérabilité existante.

Les vulnérabilités correspondent aux faiblesses ou aux lacunes permettant la compromission d'un actif (ISO/IEC, 2022b). Elles peuvent être techniques, organisationnelles, humaines ou procédurales, et se manifestent par exemple par des contrôles absents ou inefficaces, des pratiques inadéquates, un manque de formation, ou une mauvaise conception des processus (International Organization for Standardization, 2018). La compromission d'un actif peut alors affecter sa confidentialité, son intégrité ou sa disponibilité, conformément aux objectifs classiques de la sécurité de l'information (Nieles, Dempsey et Pillitteri, 2017) , mais peut également se traduire par des atteintes physiques aux personnes ou aux équipements. La gestion des risques de sécurité d'une entreprise considère tous les types de risques de sécurité sans distinction qu'ils soient physiques, cybers, informationnels ou relatifs au personnel (ASIS International, 2021).

Lorsque des mécanismes de sécurité sont mis en place, qu'il s'agisse de mesures techniques, organisationnelles ou humaines, le risque n'est généralement pas éliminé, mais réduit. Les vulnérabilités qui subsistent après l'application de ces mécanismes sont qualifiées de vulnérabilités résiduelles, et le risque associé devient un risque résiduel (NIST - Joint Task Force Transformation Initiative, 2012) . L'évaluation de ce risque résiduel constitue un élément central de la posture de sécurité d'une organisation.

Il existe plusieurs façons d'adresser un risque, notamment en l'évitant, en le réduisant, en le transférant, en le répartissant ou en l'acceptant (Garcia, 2008). Toutefois, il convient de souligner une nuance conceptuelle importante. À l'exception de l'acceptation du risque, ces stratégies n'agissent pas directement sur le risque en tant que tel, mais sur les variables qui le composent, soit la valeur des actifs, l'exposition aux menaces ou le niveau des vulnérabilités résiduelles. L'acceptation du risque correspond quant à elle à une décision explicite de ne pas intervenir sur ces variables, et donc de tolérer le niveau de risque existant (Garcia, 2008).

Dans la pratique, les vulnérabilités constituent fréquemment la variable la moins rigoureusement évaluée dans les analyses de risque. La littérature normative et scientifique souligne que les démarches d'analyse accordent souvent une attention prioritaire à l'identification des menaces et à l'estimation des impacts, tandis que les vulnérabilités sont traitées de manière incomplète, implicite ou présumée. Plusieurs cadres de gestion du risque indiquent que cette faiblesse découle notamment d'une surestimation de l'efficacité des mesures existantes, d'un manque de données objectives ou d'une évaluation insuffisamment critique des contrôles en place. Cette sous-évaluation des vulnérabilités compromet directement la validité du risque estimé et peut conduire à une perception erronée du niveau réel de sécurité, même lorsque les actifs et les menaces sont correctement identifiés (ISO/IEC, 2022b ; NIST - Joint Task Force Transformation Initiative, 2012 ; Aven, 2016 ; Anthony (Tony)Cox, 2008).

Ce constat met en évidence l'importance d'une approche de sécurité accordant une attention particulière à l'identification et à l'analyse des vulnérabilités, lesquelles jouent un rôle déterminant dans l'évaluation de la posture de sécurité globale d'une organisation.

1.2 Cadres et approches holistiques de la sécurité

La littérature scientifique suggère qu'il existe très peu de cadres de sécurité qui intègrent de manière explicite et opérationnelle la sécurité physique, la sécurité du personnel (incluant le filtrage et les vérifications d'antécédents) ainsi que la sécurité de l'information ou la cybersécurité au sein d'une méthodologie organisationnelle unique et cohérente. Bien que plusieurs cadres de gouvernance et de gestion des risques revendiquent une portée holistique ou globale, leur mise en œuvre concrète demeure largement centrée sur la cybersécurité et les systèmes d'information.

Melaku (2023) observe que, même au sein de modèles de gouvernance de la cybersécurité présentés comme stratégiques ou organisationnels, la sécurité physique et la sécurité du personnel sont le plus souvent traitées comme des considérations périphériques ou comme des

éléments contextuels implicites, plutôt que comme des domaines pleinement intégrés et analysés sur un pied d'égalité. Il en résulte des cadres qui tendent à renforcer une vision fragmentée de la sécurité organisationnelle, dans laquelle les risques numériques sont systématiquement priorisés, tandis que les dimensions humaines et physiques demeurent insuffisamment formalisées et intégrées sur le plan méthodologique. D'un autre côté, Raufi et Usmani (2024) expliquent que la sécurité physique seule est insuffisante pour protéger des actifs numériques et informationnels dans un environnement connecté. Bien que cette observation confirme l'importance d'une approche intégrée de la sécurité, plusieurs observations terrain indiquent qu'en pratique, les organisations tendent à concentrer leurs efforts principalement sur la cybersécurité.

Bien que des auteurs tels que Šarūnas Grigaliūnas et al. (2024) reconnaissent explicitement que la sécurité des organisations ne peut plus être abordée selon une logique de silos, et qu'ils soulignent l'interdépendance entre les systèmes techniques, les personnes et l'environnement organisationnel, leurs travaux ne proposent pas pour autant une méthodologie intégrée et globale des différents domaines de la sécurité. Ces approches ne présentent pas de cadre structuré permettant d'analyser simultanément la sécurité physique, le filtrage de sécurité des personnes (incluant les enjeux liés aux ressources humaines et aux menaces internes) et la cybersécurité au sein d'un même dispositif analytique. Il s'agit plutôt d'une démarche conceptuelle et analytique, certes plus large que les approches strictement cybercentrées, mais demeurant incomplète du point de vue opérationnel. En ce sens, ces travaux contribuent à la reconnaissance du caractère systémique de la sécurité organisationnelle, sans toutefois offrir un cadre ou un outil directement mobilisable pour l'évaluation concrète de la posture de sécurité globale sur le terrain.

Cette limite est également observée dans la littérature portant sur les systèmes cyber-physiques, où la convergence entre sécurité (security) et sûreté (safety) est de plus en plus discutée. Kavallieratos, Katsikas et Gkioulos (2020), dans une revue exhaustive des travaux sur le co-engineering de la cybersécurité et de la sûreté des systèmes cyber-physiques, soulignent que l'interdépendance entre composantes numériques et physiques rend les approches

traditionnelles en silo théoriquement et pratiquement insuffisantes. Les auteurs reconnaissent explicitement que des incidents de cybersécurité peuvent entraîner des impacts physiques majeurs et, inversement, que des défaillances physiques peuvent exposer des vulnérabilités cyber. Cette reconnaissance confirme le caractère systémique de la sécurité dans les environnements organisationnels complexes.

Toutefois, malgré cette prise de conscience largement partagée, Kavallieratos et al. (2020) constatent que les approches recensées demeurent majoritairement partielles, théoriques ou limitées à des contextes techniques spécifiques, notamment industriels ou embarqués. Les cadres analysés se concentrent essentiellement sur l'ingénierie des systèmes et sur l'intégration des dimensions cyber et physiques, sans proposer de méthodologie organisationnelle globale intégrant explicitement la sécurité physique, la sécurité du personnel et la cybersécurité dans un dispositif analytique unique et applicable sur le terrain. À l'instar des approches précédemment évoquées, ces travaux mettent en évidence la nécessité d'une vision intégrée de la sécurité, tout en illustrant l'absence persistante d'outils structurés permettant d'évaluer concrètement et simultanément l'ensemble des domaines de la sécurité organisationnelle au sein des entreprises.

En matière d'infrastructures essentielles, les travaux associés à la Critical Information Infrastructure Protection (CIIP), parfois désignés sous l'appellation Integrated CIIP (ICIIP), reconnaissent explicitement l'interdépendance entre systèmes techniques, infrastructures et mécanismes organisationnels de sécurité (Dunn Cavelty, 2009 ; Klimburg, 2012). Cependant, la provenance et le titre même du document du NATO Cooperative Cyber Defense Centre of Excellence Tallinn, Estonia qui « National Cyber Security Framework Manual » édité par Klimburg (2012) témoignent une fois de plus du focus toujours mis sur la cybersécurité. De plus, ces approches demeurent essentiellement conceptuelles et orientées vers la gouvernance stratégique. Elles ne proposent pas de méthodologie structurée permettant d'analyser simultanément, sur le terrain, la sécurité physique, le filtrage de sécurité des personnes et la cybersécurité au sein des organisations.

Dans l'ensemble, la prise en compte des vulnérabilités nécessite une approche holistique intégrant le renforcement technique, l'adoption de politiques organisationnelles robustes, la mise en place de contrôles procéduraux rigoureux, ainsi qu'une attention particulière portée au facteur humain par la formation et la sensibilisation à la sécurité. Cette approche multidisciplinaire est essentielle pour développer des mécanismes de protection adaptatifs et proactifs face à l'évolution des menaces, et pour réduire le risque de compromission des actifs (Mohamed, A. Hefny et R. Darwish, 2024 ; Isparta University of Applied Sciences, Department of Information Security, Isparta, Turkey et Süzen, 2020 ; Ijiga *et al.*, 2025 ; Djenna, Harous et Saidouni, 2021).

1.3 Cadres, normes et méthodologies par domaine

Comme présenté précédemment, plusieurs approches contemporaines de la sécurité soulignent l'importance d'adopter une vision globale et multidimensionnelle de la protection des organisations. Toutefois, malgré cette volonté d'intégration, la littérature ainsi que les pratiques organisationnelles démontrent que les différents domaines de sécurité continuent généralement d'être structurés, encadrés et développés de manière relativement indépendante. Les cadres normatifs, les méthodologies et les référentiels existants demeurent ainsi fortement spécialisés selon les disciplines concernées, notamment en cybersécurité, en sécurité physique ou en filtrage de sécurité.

Cette réalité contribue à maintenir certaines approches en silo où les mécanismes de protection, les méthodes d'analyse ainsi que les objectifs de sécurité sont souvent abordés séparément selon les expertises et les secteurs d'activité. De plus, l'analyse de la littérature révèle l'absence apparente de cadre universel permettant d'intégrer uniformément l'ensemble des dimensions de la sécurité organisationnelle à l'intérieur d'une même méthodologie structurée.

Dans ce contexte, il apparaît pertinent d'examiner les principaux cadres, normes et méthodologies propres à chacun des domaines étudiés dans le cadre de cette recherche. Les sections suivantes présentent donc un survol des principales approches associées au filtrage de

sécurité, à la sécurité physique ainsi qu'à la cybersécurité afin de mieux comprendre leurs caractéristiques, leurs limites et leurs niveaux d'intégration respectifs.

1.3.1 Le filtrage de sécurité

Le filtrage de sécurité constitue l'une des composantes fondamentales de la protection de l'information et des actifs organisationnels. Dans plusieurs organisations, particulièrement celles œuvrant dans des secteurs sensibles ou manipulant de l'information stratégique, le filtrage de sécurité vise principalement à évaluer la fiabilité, l'intégrité et le niveau de confiance pouvant être accordé à une personne avant qu'elle n'obtienne un accès à des actifs, des installations ou des informations sensibles (Amsel et Amsel, 1989 ; ASIS International, 2021).

Le concept de filtrage de sécurité englobe généralement un ensemble de processus organisationnels permettant de vérifier les antécédents, les références, la situation financière, les affiliations, le parcours professionnel ou certains comportements pouvant représenter un risque pour l'organisation. Selon les contextes organisationnels et gouvernementaux, ces processus peuvent inclure des vérifications judiciaires, des enquêtes administratives, des validations d'identité, des entrevues de sécurité, des vérifications de crédit ou encore des enquêtes de voisinage (Service canadien du renseignement de sécurité, 2018 ; ASIS International, 2021).

Dans les milieux gouvernementaux et les infrastructures critiques, le filtrage de sécurité est fréquemment intégré à des programmes formels d'habilitation de sécurité permettant de classifier les accès selon différents niveaux de sensibilité (Service canadien du renseignement de sécurité, 2018). Cette approche repose sur le principe selon lequel certaines menaces proviennent non seulement d'acteurs externes, mais également d'individus disposant d'un accès légitime aux systèmes, aux installations ou à l'information. Les menaces internes, qu'elles soient intentionnelles ou non intentionnelles, représentent d'ailleurs une

préoccupation croissante dans la littérature portant sur la sécurité organisationnelle et la sécurité de l'information (Greitzer et Frincke, 2010 ; Colwill, 2009).

La littérature portant sur le filtrage de sécurité des employés met en évidence une importante variabilité des pratiques et des méthodologies utilisées selon les contextes organisationnels et réglementaires. Bien que plusieurs approches de vérification préalable à l'embauche existent, les travaux recensés ne permettent pas d'identifier un cadre universel, intégré et largement reconnu pour le filtrage de sécurité des employés au sein des PME (Rushchenko, Rushchenko et Plakhova, 2020).

1.3.2 La sécurité physique

La littérature portant sur la sécurité physique comprend plusieurs cadres normatifs, méthodologies d'analyse et approches opérationnelles utilisés dans différents secteurs d'activité. Parmi les principaux référentiels recensés figurent notamment :

- Protection of Assets (ASIS International)
- Physical Asset Protection Standard
- General Security Risk Assessment Guideline
- NFPA 730 – Guide for Premises Security
- NFPA 731 – Standard for the Installation of Electronic Premises Security Systems
- UL 2050 – National Industrial Security Systems
- Crime Prevention Through Environmental Design (CPTED)
- Defense-in-Depth
- Layered Security
- Threat-Vulnerability-Asset (TVA) Methodology
- Security-in-Depth
- Enterprise Security Risk Management (ESRM)
- Physical-Cyber Security Convergence

Ces cadres et méthodologies proviennent principalement des travaux de l'ASIS International, de l'ISO, du National Fire Protection Association (NFPA), du Department of Homeland Security (DHS), de l'International Atomic Energy Agency (IAEA) ainsi que de plusieurs auteurs spécialisés en sécurité physique et gestion des risques organisationnels (ASIS International, 2021 ; ASIS International, 2023 ; Garcia, 2008 ; Crowe, 2000 ; National Fire Protection Association, [s d]).

1.3.3 La cybersécurité

Comme il a été établi précédemment, plusieurs cadres normatifs, standards et méthodologies associent ou confondent fréquemment les concepts de cybersécurité et de sécurité de l'information. Cette réalité est particulièrement observable dans la littérature technique et normative, où plusieurs référentiels présentés comme relevant de la cybersécurité couvrent également des dimensions plus larges de la sécurité de l'information, notamment la gouvernance, les politiques organisationnelles, la gestion des accès, la continuité des activités ou encore certains aspects liés au facteur humain. Ainsi, bien que la présente section porte spécifiquement sur la cybersécurité, certains cadres recensés demeurent officiellement associés à la sécurité de l'information en raison de leur portée conceptuelle et organisationnelle.

La littérature portant sur la cybersécurité comprend un nombre important de cadres normatifs, de standards techniques, de méthodologies d'analyse et de guides de bonnes pratiques largement diffusés à l'échelle internationale. Parmi les principaux référentiels recensés figurent notamment :

- ISO/IEC 27001 – Information Security Management Systems (ISMS)
- ISO/IEC 27002 – Information Security Controls
- ISO/IEC 27005 – Information Security Risk Management
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 – Security and Privacy Controls for Information Systems
- NIST SP 800-61 – Computer Security Incident Handling Guide

- NIST SP 800-171 – Protecting Controlled Unclassified Information
- Cybersecurity Maturity Model Certification (CMMC)
- CIS Critical Security Controls
- MITRE ATT&CK Framework
- Zero Trust Architecture (NIST SP 800-207)
- CyberSecure Canada
- Programme de coordination de la cybersécurité canadienne (PCCC)
- COBIT
- SOC 2 Security Framework
- Center for Internet Security (CIS) Benchmarks

Ces cadres et méthodologies proviennent principalement des travaux de l'International Organization for Standardization (ISO), du National Institute of Standards and Technology (NIST), du Centre canadien pour la cybersécurité, du Department of Defense des États-Unis, du Center for Internet Security (CIS), du MITRE Corporation, d'ISACA ainsi que de plusieurs organisations spécialisées en gouvernance et en sécurité des technologies de l'information (International Organization for Standardization, 2018 ; ISO/IEC, 2022b ; NIST, 2013 ; U.S. Department of War, [s d] ; Center for Internet Security, [s d] ; Canada, 2022 ; ISACA, [s d] ; AICPA & CIMA, [s d]).

CHAPITRE 2

VISION D'EXPERTS SUR LA SÉCURITÉ DES PME AU QUÉBEC

Cette synthèse analyse et consolide les perspectives de huit experts reconnus dans divers domaines de la sécurité (cybersécurité, sécurité physique, sécurité incendie, filtrage de personnel et sécurité de l'information). Il s'agit de praticiens non pas de chercheurs universitaires. L'analyse révèle un consensus sur l'état de vulnérabilité critique et la piètre posture de sécurité des petites et moyennes entreprises (PME) au Québec et au Canada. La maturité en matière de sécurité des PME est jugée extrêmement faible, principalement en raison d'un manque de connaissances, de ressources (temps, argent, expertise) et d'une approche de gouvernance mal structurée.

Les experts soulignent que la sécurité est souvent perçue de manière fragmentée, réduite à un seul domaine comme la cybersécurité, au détriment d'une vision holistique. Les investissements sont massivement et de manière déséquilibrée dirigés vers des technologies et les équipements visibles (pare-feu, caméras), tandis que les processus et, surtout, le facteur humain (formation, sensibilisation, filtrage) sont gravement négligés. Le travail en silo est un problème endémique, non seulement entre les différents domaines de la sécurité (physique, cybernétique, RH), mais aussi à l'intérieur même de ces spécialités, empêchant toute intégration efficace des mesures de protection.

Il n'existe actuellement aucune norme ou outil simple, accessible et global permettant à une PME d'évaluer et de structurer sa posture de sécurité de manière intégrée. Les cadres existants (NIST, ISO) sont jugés trop complexes et inadaptés à leur réalité. La première étape fondamentale recommandée par la majorité des experts pour toute PME est de réaliser un inventaire de ses biens et actifs afin de comprendre ce qui doit être protégé et quelle en est la valeur, jetant ainsi les bases d'une véritable gestion des risques. Cependant, par la suite, les entreprises sont livrées à elles même face à des consultants ayant une vision tunnel ou pire incompétent.

Si une entreprise se fait voler:
...elle appelle un serrurier: elle aura une nouvelle serrure.
...elle appelle un spécialiste en alarmes: elle aura un système d'alarme.
...elle appelle un spécialiste en contrôle d'accès: elle aura un système de contrôle d'accès.
...elle appelle la SPCA: elle va finir avec un chien!

Francis Coats ing. PSP CISSP

2.1 Justification de la sélection des experts

Le corpus de ce travail de recherche repose, entre autres choses, sur des entretiens avec des praticiens hautement reconnus du domaine de la sécurité, et non sur des chercheurs universitaires traditionnels. Cette décision a été prise, entre autres, en cohérence avec la maxime de l'ÉTS qui est : « Le génie pour l'industrie ».

L'Absence académique dans les domaines de la sécurité

Il est généralement reconnu que les chercheurs universitaires du Québec, particulièrement en cybersécurité, sont largement absents des événements de sécurité organisés par et pour les praticiens. Cette observation est accentuée par le manque de recherche académique structurée et de formations dans des domaines cruciaux comme la sécurité physique et le filtrage de sécurité. Ces deux domaines étant souvent relégués respectivement à des sous domaines de la cybersécurité ou des ressources humaines.

Plusieurs experts consultés ont noté une déconnexion entre la théorie et la pratique:

- M. Sauvé déplore que la nouvelle génération d'académiciens, ayant "juste fait un des cours à l'université", manque souvent de l'expérience pratique nécessaire pour gérer les "vraies choses" en entreprise.
- M. Waterhouse insiste sur le fait que la montée professionnelle, surtout dans la fonction publique, favorise parfois ceux qui présentent ce qu'ils ont

appris théoriquement, mais dont la "mise en application, est limité". Il martèle que l'expertise requiert d'avoir "travaillé sur le terrain avant tout".

En conséquence, ce mémoire privilégie l'expérience acquise sur le terrain et la reconnaissance professionnelle par la communauté des praticiens, comme en témoignent les antécédents militaires, policiers, gouvernementaux ou entrepreneuriaux des personnes interrogées.

Choix des experts

Les huit personnes sélectionnées ont été choisies spécifiquement parce qu'elles sont considérées comme des figures marquantes et des acteurs reconnus de la sécurité au Québec. Le choix s'est concentré sur des individus qui non seulement possèdent une expertise technique profonde, mais qui ont également démontré leur capacité à influencer et à structurer l'industrie de la sécurité à travers leurs fonctions, leurs entreprises, leur implication communautaire ou encore leur grande présence médiatique (ex.: Hackfest, CANASA, ASIS, médiatisation).

Tableau 2.1 Profils des experts consultés

Nom de l'expert	Titre et fonction actuelle(s)	Domaine d'expertise principal(aux)
Alain Côté	Capitaine à la Sûreté du Québec à titre d'officier pour le service de filtrage de sécurité (Retraité). Ancien témoin expert pour le CRPQ.	Filtrage de sécurité et habilitations sécuritaires à différents niveaux gouvernementaux. Son expertise est reconnue dans les bases de données d'enquête et le perfectionnement des systèmes d'habilitation.
André Fiset	Directeur National (Northland Controls). Membre du Conseil national de la CANASA et d'ASIS Québec.	Sécurité physique, intégration de systèmes de sécurité. Vingt-cinq ans à la GRC, incluant la responsabilité du GTI en Ontario, et expertise dans le contournement des systèmes de sécurité.

Nom de l'expert	Titre et fonction actuelle(s)	Domaine d'expertise principal(aux)
Jacques Sauvé	Consultant en cybersécurité. Co-animateur du podcast "French Connection".	Cybersécurité défensive pour les PME (bonnes pratiques, configuration, mitigation des cyberattaques). Reconnu pour son expérience pratique de 34 ans en informatique et réseautique.
Normand Racine	Président d'une firme de consultants. Ancien chef inspecteur à la Régie du Bâtiment du Québec (RBQ).	Sécurité physique et sécurité incendie intégrées dans les bâtiments. Expertise en gestion de service de sécurité bâtimentaire pour les bâtiments critiques de l'État. Possède une formation en prévention incendie, électricité et automatisation.
Patrick Mathieu	Président (Access communication). Co-fondateur du Hackfest depuis 2009.	Sécurité applicative (logiciel), sécurité offensive. Reconnu comme une figure clé de la communauté et de la relève en cybersécurité au Québec.
Steve Waterhouse	Capitaine à la retraite. Ancien Sous-Ministre Adjoint à la Cybersécurité du Québec (MCN). Chargé de cours (Université de Sherbrooke).	Sécurité de l'information et cybersécurité. Reconnu pour avoir travaillé les 10 domaines du CISSP. Contribue largement à la démocratisation de la cybersécurité dans les médias et l'enseignement.
Éric Parent	Président fondateur d'EVA Technologie.	Cybersécurité, gestion de risques, gestion de crise. Spécialisé dans l'alignement de la sécurité avec les objectifs d'affaires et l'étude de la psychologie humaine en sécurité. Reconnu pour ses nombreuses apparitions médiatiques (plus de 1000 entrevues).

Nom de l'expert	Titre et fonction actuelle(s)	Domaine d'expertise principal(aux)
Denis Bourget	Président du chapitre du Québec de ASIS International. Directeur Général de l'Amérique du Nord (Idemia).	Sécurité physique, identification biométrique (48 ans d'expérience dans l'industrie). Reconnu pour son rôle dans la promotion des certifications ASIS pour professionnaliser l'industrie de la sécurité physique.

2.2 Introduction

La sécurité dans son ensemble n'est pas un enjeu purement technique, mais un impératifs stratégiques majeur pour la survie et la prospérité des organisations québécoises. Dans un paysage de menaces en constante évolution, la capacité à anticiper, gérer et répondre aux risques est devenue une compétence organisationnelle fondamentale. Cette synthèse a pour objectif d'articuler une vision claire des défis contemporains, de l'état de la gouvernance de la sécurité et des perspectives d'amélioration. Cette analyse s'appuie exclusivement sur une série d'entretiens menés avec des experts reconnus du secteur, dont les propos et les perspectives ont été soigneusement compilés. Les experts dont les analyses sont synthétisées dans ce document sont Alain Côté, Jacques Sauvé, Normand Racine, Patrick Mathieu, Steve Waterhouse, Éric Parent et Denis Bourget. Ce document vise à soutenir mon travail de maîtrise en présentant les résultats d'entrevues réalisées afin de définir plusieurs éléments liés à la conception d'un outil d'analyse de la posture de sécurité d'une entreprise. Ces entrevues avaient pour objectif d'identifier les points communs et les disparités entre différents domaines d'expertise, ainsi que d'évaluer les enjeux de gouvernance et les difficultés associées à la mise en place des contrôles de sécurité. Le guide d'entrevue utilisé dans le cadre de ces entretiens est présenté à ANNEXE I.

2.3 La perception et la portée de la sécurité organisationnelle

La première étape vers une posture de sécurité robuste est une définition claire et partagée de ce que la sécurité englobe. Les experts consultés s'accordent sur une vision large et intégrée, traitant la sécurité comme une discipline de gestion globale. Cependant, la réalité opérationnelle, particulièrement au sein des petites et moyennes entreprises (PME), révèle une application souvent limitée ou fragmentée, se concentrant presque exclusivement sur la cybersécurité.

Malgré la vision holistique et intégrée des experts, la perception commune au sein des organisations est beaucoup plus restrictive. Jacques Sauvé observe que pour la majorité des dirigeants, en particulier dans les PME, le terme « sécurité » est un synonyme quasi exclusif de « cybersécurité ». La discussion se concentre presque entièrement sur les menaces informatiques telles que les cyberattaques et les rançongiciels, occultant les autres dimensions critiques du risque. Cette vision tunnel conduit à une négligence dangereuse des risques liés aux facteurs physiques (accès aux locaux, protection des équipements) et humains (filtrage du personnel, menaces internes), qui sont pourtant des vecteurs d'attaque tout aussi courants et potentiellement dévastateurs. Cette perception limitée est renforcée par une méconnaissance générale des risques réels. Comme le souligne Jacques Sauvé : « You don't know what you don't know”.

Cette vision fragmentée du risque se reflète directement dans les structures de gouvernance, souvent inadéquates, qui sont observées au sein des organisations québécoises.

2.4 La gouvernance de la sécurité

La gouvernance est le pilier structurel sur lequel repose toute stratégie de sécurité efficace. Elle définit les rôles, les responsabilités et l'autorité nécessaires pour aligner les efforts de sécurité sur les objectifs stratégiques de l'organisation. Cette section analyse l'état de la gouvernance de la sécurité au Québec, exposant le fossé profond qui sépare les rôles théoriques de leadership

en sécurité de leur application concrète, ainsi que l'absence quasi totale de structure formelle dans la majorité des PME.

2.4.1 Les rôles de leadership (CSO et CISO) : ambiguïté et positionnement opérationnel

L'évaluation de l'état des rôles de Chief Security Officer (CSO) et Chief Information Security Officer (CISO) dans les organisations québécoises révèle plusieurs lacunes structurelles :

- Rareté du CSO : Le rôle de CSO, qui incarne la vision holistique de la sécurité en intégrant les volets physique, personnel et cybernétique, est très rarement implanté au Québec. Éric Parent et Denis Bourget confirment que ce poste, censé chapeauter l'ensemble des fonctions de sécurité, demeure une exception.
- Prédominance du CISO : Le rôle le plus courant est celui de CISO. Cependant, sa fonction est souvent cantonnée à la cybersécurité et positionnée de manière trop opérationnelle. Comme le notent Éric Parent et Patrick Mathieu, le CISO est fréquemment subordonné au département des technologies de l'information (TI), ce qui limite sa portée stratégique et son indépendance.
- Manque de définition : Un manque de consensus sur la définition précise des responsabilités de ces rôles mène à des interprétations très variables d'une organisation à l'autre. Éric Parent et Steve Waterhouse soulignent que cette ambiguïté empêche l'établissement de mandats clairs et d'une autorité cohérente.
- Problèmes de silos : La mauvaise structure hiérarchique et le manque de communication entre les départements (sécurité physique, TI, ressources humaines) créent des silos qui paralysent l'efficacité de la sécurité. Cette problématique est directement liée à l’absence d’une stratégie organisationnelle claire et partagée. Comme le mentionne Steve Waterhouse : « S’il y a une absence de stratégie commune à l'organisation et qu'elle est pas bien expliquée vers le bas, elle sera pas bien appliquée vers le bas... Les gens vont s'isoler. ». Patrick Mathieu analyse que, même lorsqu'un CISO est en place, il dispose rarement du pouvoir ou de l'autorité nécessaires pour influencer les pratiques des autres départements, rendant toute approche intégrée impossible.

2.4.2 La situation critique des PME : l'absence de gouvernance

La situation de la gouvernance de la sécurité est particulièrement alarmante au sein des PME, où les structures formelles sont pratiquement inexistantes.

- Absence de rôles dédiés : Les experts sont unanimes : les PME n'ont pas de postes dédiés à la sécurité. Cette responsabilité est souvent une tâche secondaire ajoutée aux fonctions d'un administrateur réseau ou d'un « homme/femme à tout faire » qui manque de temps et d'expertise (Jacques Sauvé, Steve Waterhouse).
- Dépendance externe : Le principal silo dans une PME ne se situe pas à l'interne, mais entre l'entreprise elle-même et son fournisseur de services TI externe. Éric Parent note que les PME accordent une confiance aveugle à ce partenaire, sans jamais valider la qualité ou la pertinence des services et protections mis en place. Cette dépendance est aggravée par le fait que les PME, manquant d'expertise interne, sont incapables de valider les compétences ou la performance de leurs propres fournisseurs, créant un cycle de confiance non vérifiée.
- Manque de maturité : Le niveau de maturité en gouvernance est qualifié de « proche de zéro » par Jacques Sauvé. Cette situation est caractérisée par une absence totale de documentation, de politiques de sécurité formalisées ou même de schémas de réseau de base.

  Cette faiblesse structurelle généralisée conduit inévitablement à une répartition déséquilibrée et fondamentalement réactive des efforts de sécurité.

2.5 L'asymétrie des efforts : une culture réactive face à des menaces proactives

L'analyse de la répartition des efforts et des investissements en sécurité révèle deux déséquilibres majeurs, identifiés unanimement par les experts. Le premier est une posture fondamentalement réactive, où l'action suit l'incident plutôt que de le précéder. Le second est

une sur-dépendance à la technologie, au détriment des facteurs humains et procéduraux qui sont pourtant au cœur de la plupart des failles de sécurité.

2.5.1 Priorité à la réaction plutôt qu'à la prévention

La posture opérationnelle des organisations, et plus particulièrement des PME, est majoritairement tournée vers la réaction. Les ressources (temps, argent, personnel) sont allouées pour répondre aux incidents après qu'ils se sont produits, plutôt que pour les empêcher. Steve Waterhouse et Jacques Sauvé observent que les PME concentrent leurs efforts sur le dernier verbe d'action de la gestion de crise , « répondre » ou « récupérer », n'agissant qu'après avoir été victimes d'une attaque. Cette approche s'apparente à « éteindre le feu » plutôt qu'à construire une structure ignifuge dès le départ, un modèle non viable face à des menaces de plus en plus sophistiquées et proactives.

2.5.2 Le déséquilibre des investissements : technologie, processus et humain

Les investissements en sécurité devraient être répartis de manière équilibrée entre les trois leviers que sont la technologie, les processus et le facteur humain. Or, les experts constatent une asymétrie flagrante comme le présente le Tableau 2.2.

Tableau 2.2 Déséquilibre des investissements en sécurité selon les leviers organisationnels

Levier d'investissement	**État de la situation selon les experts**
Technologie & équipements	**Sur-investi**. Les organisations, et surtout les PME, achètent des « solutions magiques » et des « patentes à gosses » vendues par des fournisseurs. Cet investissement crée un faux sentiment de sécurité (Jacques Sauvé, Steve Waterhouse, Éric Parent, Normand Racine).

Levier d'investissement	**État de la situation selon les experts**
Processus & politiques	**Sous-investi.** Les procédures pour supporter la technologie sont souvent inexistantes, incomplètes ou non suivies. La documentation est quasi absente dans les PME (Jacques Sauvé, Patrick Mathieu). Le gouvernement, à l'inverse, est parfois paralysé par un excès de procédures sans exécution (Patrick Mathieu).
Facteur humain (sensibilisation & formation)	**Gravement négligé.** La sensibilisation des employés est considérée comme la dernière roue du carrosse. L'humain est vu comme le maillon faible mais reçoit le moins d'attention et d'investissement (Jacques Sauvé, Alain Côté, Patrick Mathieu, Denis Bourget).

Cette répartition des ressources est profondément inefficace, car en sur-investissant dans la technologie, les organisations négligent les deux vecteurs d'attaque que les experts identifient comme les plus critiques : le facteur humain (dont l'erreur humaine) et les processus défaillants. Cette incohérence dans les investissements est également observée dans la gestion des accès et des responsabilités. Comme le souligne Alain Côté : « Ils vont engager une compagnie pour venir installer des systèmes d'alarme, ils vont mettre des sécurités, des pare-feu, toutes sortes de choses sur le système, mais à qui il donne les clés? » De plus, un pare-feu de pointe ne sert à rien si un employé non sensibilisé clique sur un lien d'hameçonnage ou si les procédures de mise à jour ne sont pas suivies. Ce n'est donc pas juste l'absence de procédures, mais également leur non-application. Alain Côté souligne également que : « Même s'il y a des règles qui étaient là en bien des endroits, les gens ne les suivent pas, ils n'appliquent pas les règles [...] puis c'est là qu'il y a des bris de sécurité. »

Cette culture réactive est maintenue en place par une série d'obstacles bien réels qui empêchent spécifiquement les PME de structurer leur approche.

2.6 Obstacles majeurs à la structuration de la sécurité dans les PME

La faible maturité en sécurité des PME québécoises n'est pas le fruit du hasard, mais le résultat d'une série d'obstacles interconnectés qui freinent l'adoption d'une approche plus structurée. Les experts ont identifié plusieurs freins majeurs qui maintiennent ces organisations dans un cycle réactif et vulnérable.

1. Le manque de conscience et de compréhension du risque L'obstacle le plus fondamental est que les dirigeants de PME ne comprennent pas la nature du risque de sécurité. Comme le résume Jacques Sauvé : "you don't know what you don't know". Le risque est perçu comme quelque chose de « virtuel » et de lointain jusqu'à ce qu'un incident se produise et matérialise la menace de manière brutale (Éric Parent, Patrick Mathieu). Cette absence de conscience empêche de considérer la sécurité comme une priorité stratégique.
2. Les contraintes de coût, de temps et de ressources La sécurité est perçue comme un centre de coût pur, sans retour sur investissement tangible. Alain Côté évoque la « pensée magique » selon laquelle une sécurité robuste peut être obtenue pour presque rien. En parallèle, comme le souligne Éric Parent, les PME doivent concentrer leurs ressources limitées sur leurs opérations principales pour assurer leur survie, reléguant la sécurité au bas de la liste des priorités.
3. L'absence d'expertise interne et de confiance externe Les PME font face à un dilemme : elles ne disposent pas des experts nécessaires à l'interne pour gérer leur sécurité, mais elles peinent également à évaluer la compétence des fournisseurs externes. Patrick Mathieu et Steve Waterhouse expliquent que ce manque de discernement les rend vulnérables à des vendeurs qui proposent des solutions technologiques inadaptées ou surdimensionnées, créant un faux sentiment de sécurité sans adresser les risques réels.

4. La complexité des cormes et le manque de guides adaptés Les cadres de référence existants, tels que NIST ou les normes ISO, sont jugés trop complexes, lourds et coûteux pour être applicables par une PME (Patrick Mathieu, Steve Waterhouse). Les experts comme Denis Bourget et Éric Parent déplorent l'absence d'un outil ou d'une norme globale et simplifiée qui pourrait guider une PME de manière holistique et pragmatique dans la mise en place de sa sécurité.
5. Les failles systémiques et réglementaires des défis structurels viennent compliquer la tâche des PME. Alain Côté mentionne les « trous dans le système » de vérification des antécédents, où des juridictions non communicantes ou des failles procédurales passées ont permis à des individus d'éviter la création d'un casier judiciaire malgré des infractions. De plus, la complexité de certaines réglementations, comme la Loi 25, peut paraître insurmontable et inadaptée au contexte opérationnel et aux ressources d'une petite entreprise (Denis Bourget).

Malgré ces obstacles importants, les experts s'accordent sur le fait que des pistes d'amélioration concrètes et accessibles existent pour permettre aux PME de renforcer significativement leur posture de sécurité.

2.7 Vers une posture de sécurité renforcée : perspectives et recommandations stratégiques

L'objectif pour une organisation, en particulier une PME, n'est pas d'atteindre une sécurité parfaite et infaillible, mais plutôt d'amorcer un cycle d'amélioration continue en se concentrant sur les actions pragmatiques ayant le plus grand impact. Les experts proposent une feuille de route claire, basée sur des principes fondamentaux et des actions prioritaires accessibles.

2.7.1 Le point de départ : évaluer le risque et connaître ses actifs

La première étape, recommandée unanimement par l'ensemble des experts, est de savoir ce que l'on doit protéger. Sans cette connaissance fondamentale, tout effort de sécurité est un coup d'épée dans l'eau.

- Faire l'inventaire : Il est impératif de dresser un inventaire de ses actifs critiques. Comme le recommande Patrick Mathieu, cet inventaire doit être complet et inclure les actifs informationnels (données clients, propriété intellectuelle), physiques (serveurs, équipements de production) et humains (employés clés).
- Évaluer les postes et les risques : Une fois les actifs identifiés, il faut adopter une approche basée sur le risque. Alain Côté insiste sur la nécessité d'évaluer la sensibilité de chaque poste et de chaque actif, afin d'appliquer des mesures de sécurité proportionnées plutôt que des contrôles uniformes et coûteux qui ne sont pas justifiés partout.

2.7.2 Les actions prioritaires : hygiène de base et cadres simplifiés

Avec une compréhension claire des risques, les PME peuvent entreprendre des actions concrètes qui éliminent une grande partie des menaces à faible coût.

- L'hygiène numérique fondamentale : Patrick Mathieu souligne que trois mesures de base permettent de se prémunir contre la majorité des attaques opportunistes :
  1. Faire systématiquement les mises à jour des logiciels et systèmes.
  2. Utiliser un gestionnaire de mots de passe pour créer et gérer des mots de passe uniques et robustes.
  3. Activer l'authentification à deux facteurs (2FA) partout où elle est disponible.
- Adopter un cadre de référence accessible : Plutôt que de se perdre dans des normes complexes, les experts recommandent des cadres spécifiquement adaptés aux PME :
  - Le programme Cybersecure Canada (CAN/CIOSC 104) est décrit par Jacques Sauvé et Steve Waterhouse comme une excellente norme de base, développée spécifiquement pour les petites et moyennes organisations canadiennes.
  - Le modèle CMMC (Cybersecurity Maturity Model Certification) Niveau 1, suggéré par Éric Parent, offre un point de départ simple et une approche progressive basée sur les contrôles fondamentaux du NIST.

2.7.3 Le pilier du succès : le facteur humain et la culture de sécurité

La technologie et les processus ne sont rien sans l'implication des individus. Le facteur humain est au cœur de la réussite de toute stratégie de sécurité.

- L'impulsion par la direction : La sécurité doit être une priorité portée par la haute direction. Jacques Sauvé affirme que si le PDG ne comprend pas et ne promeut pas son importance, tout effort est voué à l'échec. Le leadership doit donner l'exemple.
- La sensibilisation continue : Pour être efficace, la sensibilisation ne doit pas être un événement ponctuel, mais doit s'intégrer dans la culture d'entreprise comme une « conversation corporative continue ». Steve Waterhouse et Denis Bourget expliquent que c'est en intégrant la sécurité dans la culture quotidienne que les employés cessent d'être le maillon faible pour devenir la première et la plus efficace ligne de défense.

En définitive, la voie vers une meilleure sécurité pour les PME passe par une prise de conscience des dirigeants, l'adoption de bonnes pratiques de base et l'instauration d'une véritable culture de la sécurité menée par l'exemple.

2.8 Conclusion

Ce dossier de synthèse, basé sur les témoignages croisés d'experts reconnus, dresse un portrait clair de l'état de la sécurité au Québec. Le constat principal est qu'un important déficit de maturité persiste, particulièrement au sein des PME. Celles-ci sont prises dans un cycle réactif, avec une vision fragmentée de la sécurité, une gouvernance quasi inexistante, et des investissements déséquilibrés qui privilégient la technologie au détriment des processus et du facteur humain. Les obstacles, manque de conscience du risque, contraintes de ressources et complexité des normes, sont réels mais non insurmontables. Le passage d'une culture réactive et technocentrée à une approche proactive, holistique et centrée sur la gestion du risque est la condition essentielle pour permettre aux organisations québécoises de naviguer avec succès dans le paysage des menaces actuel et futur.

CHAPITRE 3

MÉTHODOLOGIE

Le présent chapitre décrit la démarche méthodologique adoptée pour développer et valider l'outil d'analyse de la posture de sécurité globale proposé dans ce mémoire. Après avoir exposé, au chapitre 1, l'état des connaissances et les lacunes identifiées dans la littérature, puis présenté, au chapitre 2, les résultats des entrevues réalisées auprès de praticiens, ce chapitre précise la logique de recherche, les choix méthodologiques et les étapes de validation de l'outil.

La méthodologie repose sur trois composantes principales. La première présente la posture méthodologique et la stratégie de recherche adoptées. La deuxième décrit la démarche de structuration conceptuelle ayant conduit à la construction de l'architecture d'analyse. La troisième expose le processus de validation empirique et professionnelle de l'approche proposée.

3.1 Posture méthodologique et stratégie de recherche

La présente recherche adopte une démarche qualitative et appliquée, orientée vers la conception d'un cadre d'analyse structurant destiné aux petites et moyennes entreprises. Elle ne vise pas à produire une modélisation statistique généralisable à l'ensemble des organisations, mais à développer une architecture méthodologique cohérente permettant d'intégrer différentes dimensions de la sécurité au sein d'un outil opérationnel.

Le positionnement épistémologique retenu s'inscrit dans une logique pragmatique. L'objectif n'est pas uniquement d'enrichir le corpus théorique, mais de répondre à un problème concret identifié tant dans la littérature que dans la pratique professionnelle : l'absence d'un mécanisme intégré permettant d'évaluer de manière structurée la posture de sécurité globale d'une PME. La démarche repose sur une articulation progressive entre trois niveaux d'analyse.

Premièrement, une analyse documentaire approfondie, présentée au chapitre 1, permet de situer l'objet d'étude dans l'état des connaissances. Cette revue met en évidence la fragmentation des cadres conceptuels entre cybersécurité, sécurité physique et filtrage de sécurité des personnes. Elle révèle également une surreprésentation de la cybersécurité dans les publications récentes, ainsi qu'une tendance à assimiler la sécurité de l'information à la seule protection des technologies de l'information. Ces constats théoriques soulignent l'absence d'outils réellement intégrés couvrant l'ensemble des dimensions pertinentes pour une PME.

Deuxièmement, une série d'entrevues qualitatives, présentée au chapitre 2, permet de confronter ces constats théoriques aux réalités du terrain. Les praticiens consultés occupent des fonctions stratégiques ou opérationnelles dans différents domaines de la sécurité. Leur contribution permet d'identifier les déséquilibres observés dans les organisations, notamment la prédominance des investissements technologiques, la faible formalisation des procédures et l'insuffisance des mécanismes de sensibilisation et de formation. Les entrevues confirment également la difficulté, pour les dirigeants de PME, d'obtenir une vue d'ensemble synthétique et intelligible de leur posture de sécurité.

Troisièmement, à partir de ces constats convergents, la recherche adopte une stratégie de conception structurée visant à développer un cadre analytique intégré. Cette stratégie repose sur deux principes fondamentaux :

- l'harmonisation conceptuelle des cadres existants afin de dégager des catégories transversales communes aux différents domaines de la sécurité ;
- la structuration de ces catégories au sein d'une architecture simple, cohérente et applicable dans un contexte de ressources limitées.

La démarche méthodologique ne consiste donc pas à appliquer mécaniquement un référentiel existant, mais à procéder à une intégration raisonnée des connaissances issues de plusieurs disciplines. Elle s'appuie sur une logique d'abstraction progressive : à partir des concepts

spécifiques à chaque domaine, il s'agit d'identifier des invariants fonctionnels permettant une structuration commune.

Le choix d'une approche qualitative appliquée se justifie par la nature du problème étudié. La posture de sécurité globale d'une organisation ne se réduit pas à des indicateurs quantitatifs isolés ; elle repose sur des interactions complexes entre technologies, procédures et comportements humains. Une compréhension fine de ces interactions nécessite une démarche interprétative et structurante plutôt qu'un traitement statistique.

En résumé, la stratégie de recherche adoptée repose sur :

- une analyse critique de la littérature afin d'identifier les lacunes conceptuelles ;
- une confrontation empirique par entrevues pour valider les constats théoriques ;
- une démarche d'intégration conceptuelle visant à structurer un cadre d'analyse cohérent ;
- une validation empirique subséquente de la structure développée.

Cette posture méthodologique assure que le cadre proposé repose à la fois sur des fondements théoriques solides et sur une pertinence opérationnelle démontrée.

3.2 Démarche de structuration conceptuelle et construction de l'architecture d'analyse

La conception d'un outil d'analyse intégré en matière de sécurité organisationnelle nécessite une démarche méthodique permettant de structurer des concepts issus de disciplines distinctes. Les chapitres précédents ont mis en évidence la fragmentation des approches entre cybersécurité, sécurité physique et filtrage de sécurité des personnes, ainsi que l'absence d'un cadre synthétique adapté aux contraintes des petites et moyennes entreprises.

La présente section décrit la méthode retenue pour organiser, comparer et structurer les mécanismes de protection existants afin d'aboutir à une architecture d'analyse cohérente.

3.2.1 Recensement et extraction des cadres existants

La première étape consiste à identifier les référentiels et cadres analytiques pertinents dans les différents domaines de la sécurité organisationnelle. Cette recension inclut notamment :

- les référentiels en cybersécurité ;
- les cadres conceptuels en sécurité physique ;
- les approches en filtrage de sécurité des personnes ;
- les modèles liés à la gestion des incidents et à la continuité des affaires.

Pour chacun de ces domaines, la méthodologie prévoit une extraction systématique des catégories utilisées pour classifier les contrôles ou mécanismes de protection. Cette extraction porte sur :

- les typologies de contrôles ;
- les classifications fonctionnelles ;
- les séquences d'intervention décrites ;
- les distinctions temporelles entre prévention, gestion d'incident et rétablissement.

L'objectif de cette étape est de constituer un inventaire structuré des catégories conceptuelles utilisées dans chaque discipline, sans encore chercher à les fusionner.

3.2.2 Analyse comparative et mise en correspondance

À partir de l'inventaire constitué, une analyse comparative est réalisée. Cette analyse vise à examiner :

- les similitudes terminologiques entre domaines ;
- les différences de portée conceptuelle ;
- les recouvrements partiels ;
- les divergences structurelles.

La comparaison s'effectue sous forme de tableaux de correspondance permettant de mettre en parallèle les catégories issues des différents référentiels.

Cette étape ne consiste pas à établir immédiatement des équivalences définitives, mais à documenter les convergences et les tensions conceptuelles. Elle permet d'identifier les zones où une harmonisation est envisageable et celles où des distinctions doivent être maintenues.

Le principe directeur de cette analyse est la cohérence fonctionnelle : les catégories sont examinées en fonction de leur rôle opérationnel plutôt que de leur terminologie propre.

3.2.3 Définition des critères de structuration

Sur la base de l'analyse comparative, la méthodologie prévoit la définition de critères permettant de structurer une architecture intégrée.

Les critères retenus doivent répondre aux exigences suivantes :

- Applicabilité interdisciplinaire : la structure doit pouvoir intégrer des mécanismes provenant de plusieurs domaines sans distorsion conceptuelle.
- Simplicité opérationnelle : l'architecture doit être compréhensible par des dirigeants de PME ne disposant pas nécessairement d'une expertise spécialisée.
- Capacité de mise en évidence des déséquilibres : la structure doit permettre d'identifier les lacunes systémiques.
- Neutralité normative : l'outil ne doit pas reproduire intégralement un référentiel spécifique, mais proposer une organisation transversale.

Ces critères servent de filtres pour l'élaboration des catégories structurantes ultérieures.

3.2.4 Détermination de l'unité d'analyse

Parallèlement au travail d'harmonisation, il est nécessaire de définir l'unité à partir de laquelle l'analyse sera structurée.

Deux approches sont examinées :

- une structuration centrée sur un inventaire global de contrôles ;
- une structuration centrée sur des événements indésirables ou scénarios de risque.

Une analyse des avantages et limites de chacune de ces approches est réalisée. Les éléments comparés incluent :

- la capacité d'appropriation par les dirigeants ;
- la facilité de contextualisation ;
- la cohérence avec une logique décisionnelle ;
- la possibilité de structuration systémique.

Le choix méthodologique repose sur la capacité de l'unité retenue à assurer un arrimage entre compréhension organisationnelle et architecture analytique.

3.2.5 Organisation des mécanismes de protection

Une fois l'unité d'analyse déterminée, la méthodologie prévoit d'associer à chaque unité un ensemble de mécanismes de protection issus des différents domaines recensés.

Ces mécanismes sont sélectionnés selon des critères explicites :

- pertinence pour le contexte des PME ;
- clarté opérationnelle ;
- compatibilité avec les catégories structurantes définies précédemment.

Chaque mécanisme est ensuite classifié selon la structure retenue, permettant d'organiser les contrôles de manière systémique plutôt que cumulative.

3.2.6 Formalisation d'une architecture d'analyse

La dernière étape méthodologique consiste à formaliser l'architecture résultant du travail d'harmonisation et de classification.

Cette formalisation doit permettre :

- une représentation synthétique des mécanismes de protection ;
- une lecture transversale des différentes dimensions ;
- une identification visuelle des déséquilibres potentiels.

L'architecture retenue constitue le cadre analytique qui sera détaillé au chapitre suivant.

3.3 Validation empirique et professionnelle de l'approche proposée

La validation intégrée à la démarche méthodologique ne vise pas à tester l'exhaustivité des listes de contrôles associées aux différents événements d'exception. Elle porte principalement sur deux dimensions centrales :

- la pertinence du principe d'approche holistique ;
- la clarté et l'intelligibilité de la représentation synthétique de la posture de sécurité.

L'objectif est de vérifier si la structure développée permet effectivement d'intégrer plusieurs domaines de la sécurité dans une architecture cohérente et si le résultat obtenu est compréhensible et exploitable par des décideurs non spécialistes.

3.3.1 Validation du principe holistique

La première dimension évaluée concerne la validité du cadre intégrateur. Il s'agit d'examiner si l'architecture d'analyse permet réellement de dépasser la fragmentation observée entre cybersécurité, sécurité physique et filtrage de sécurité.

Les participants à la validation sont invités à analyser la structure proposée et à se prononcer sur :

- sa capacité à intégrer des mécanismes provenant de domaines distincts ;
- l'équilibre entre dimensions technologiques, procédurales et humaines ;

- la pertinence d'une approche croisant plusieurs fonctions de protection.

L'objectif n'est pas de valider chaque contrôle individuellement, mais d'évaluer la cohérence systémique de la structure et sa capacité à révéler des déséquilibres organisationnels.

3.3.2 Validation de la compréhension et de l'interprétation

La deuxième dimension de validation porte sur la représentation finale de la posture de sécurité.

Les participants appliquent l'architecture à leur organisation et analysent la représentation synthétique obtenue. L'évaluation porte sur :

- la facilité de lecture du résultat ;
- la capacité à identifier rapidement des lacunes ;
- la pertinence perçue de la visualisation pour soutenir la prise de décision.

Une attention particulière est portée à la capacité du modèle à produire une vue d'ensemble compréhensible sans nécessiter une expertise technique avancée.

Cette étape vise à vérifier que l'outil remplit sa fonction première : offrir une perspective globale permettant d'orienter des décisions stratégiques.

3.3.3 Portée et limites de la divulgation

Pour des raisons liées à la protection du savoir-faire et à des considérations de nature commerciale, la liste détaillée des événements indésirables ainsi que l'inventaire complet des contrôles associés ne sont pas reproduits dans le présent mémoire.

La validation porte donc sur la structure méthodologique générale et sur le mécanisme d'évaluation de la posture de sécurité, plutôt que sur le contenu exhaustif des listes opérationnelles.

Cette limitation ne compromet pas la valeur académique de la recherche, dans la mesure où l'objectif du mémoire consiste à démontrer :

- la cohérence de l'architecture d'analyse ;
- la validité du principe d'intégration interdisciplinaire ;
- la pertinence de la représentation synthétique proposée.

Le cadre méthodologique et la logique de structuration sont pleinement exposés, permettant au lecteur d'en comprendre les fondements et d'en évaluer la rigueur.

CHAPITRE 4

CONCEPTION DE L'OUTIL

Le chapitre précédent a présenté la démarche méthodologique adoptée pour structurer et développer un cadre d'analyse intégré de la posture de sécurité organisationnelle. Cette démarche reposait notamment sur une analyse comparative des cadres conceptuels existants, suivie d'un processus d'harmonisation visant à identifier des catégories analytiques transversales applicables à plusieurs domaines de la sécurité.

Le présent chapitre expose l'architecture résultant de ce processus de structuration conceptuelle. Il décrit les principes ayant guidé la conception de l'outil d'analyse ainsi que la manière dont les mécanismes de protection peuvent être organisés et interprétés dans une perspective systémique.

L'objectif n'est pas de proposer un inventaire exhaustif de contrôles de sécurité ni de reproduire un référentiel normatif existant. Il s'agit plutôt de formaliser une architecture d'analyse permettant d'intégrer, dans un cadre cohérent et lisible, différentes dimensions de la sécurité organisationnelle pertinentes pour le contexte des petites et moyennes entreprises.

Le chapitre présente d'abord les principes directeurs ayant orienté la conception de l'architecture analytique. Il décrit ensuite la structure du modèle d'analyse et la manière dont les mécanismes de protection peuvent y être organisés afin de produire une représentation synthétique de la posture de sécurité d'une organisation.

4.1 Principes directeurs de l'architecture retenue

Le développement d'une architecture d'analyse de la posture de sécurité globale nécessite l'établissement de principes directeurs permettant d'assurer la cohérence, la robustesse et la pertinence du modèle proposé. Ces principes servent de fondement conceptuel à la structure

présentée dans les sections subséquentes et orientent la manière dont les mécanismes de protection seront catégorisés et analysés.

Les principes exposés dans cette section visent à guider la conception du modèle tout en assurant que celui-ci demeure pertinent malgré l'évolution des technologies, des menaces et des pratiques organisationnelles.

4.1.1 Principe d'intégration interdisciplinaire

La sécurité organisationnelle est généralement abordée à travers plusieurs disciplines distinctes, notamment la cybersécurité, la sécurité physique et le filtrage de sécurité des personnes. Chacune de ces disciplines possède ses propres pratiques professionnelles, ses cadres conceptuels et ses terminologies.

Cette segmentation peut conduire à une gestion en silos dans laquelle les mécanismes de protection sont déployés et analysés indépendamment les uns des autres. Une telle approche complique l'obtention d'une vision globale de la posture de sécurité d'une organisation et peut conduire à une perception fragmentée des vulnérabilités.

L'architecture d'analyse développée dans ce mémoire repose donc sur un principe d'intégration interdisciplinaire. Elle vise à structurer les mécanismes de protection selon des catégories analytiques transversales applicables à plusieurs domaines de la sécurité. Cette approche permet d'intégrer dans un même cadre d'analyse des contrôles provenant de différentes disciplines tout en facilitant une compréhension globale de leur contribution à la posture de sécurité organisationnelle.

4.1.2 Principe d'équilibre systémique

L'efficacité d'un dispositif de sécurité ne repose pas uniquement sur la quantité ou la sophistication des mécanismes de protection déployés. Elle dépend également de l'équilibre entre les différentes composantes du système de sécurité.

Dans la pratique, les organisations ont souvent tendance à concentrer leurs investissements sur certaines catégories de contrôles, en particulier les solutions technologiques. Cette approche peut conduire à une sous-représentation d'autres mécanismes essentiels, tels que les procédures organisationnelles ou les mesures liées au facteur humain.

Un système de sécurité déséquilibré peut ainsi présenter des vulnérabilités importantes malgré la présence de contrôles sophistiqués dans certains domaines. L'architecture d'analyse proposée doit donc permettre d'identifier les déséquilibres potentiels entre les différentes catégories de mécanismes de protection afin de favoriser une approche plus systémique de la sécurité organisationnelle.

4.1.3 Principe de cohérence fonctionnelle

Les mécanismes de sécurité n'interviennent pas tous au même moment dans le cycle d'un incident. Certains visent à empêcher la survenue d'un événement indésirable, tandis que d'autres permettent d'en détecter l'occurrence, d'en ralentir la progression ou d'en atténuer les conséquences.

Une architecture d'analyse pertinente doit refléter cette dynamique fonctionnelle. Elle doit permettre d'évaluer si l'organisation dispose de mécanismes couvrant les différentes fonctions nécessaires à une protection efficace.

En l'absence de cette cohérence fonctionnelle, un dispositif de sécurité peut présenter des lacunes importantes. Par exemple, des mécanismes de détection performants peuvent s'avérer insuffisants si aucune capacité de réponse n'est prévue. De la même manière, des mesures préventives peuvent être contournées si aucun mécanisme ne permet de détecter ou de retarder une intrusion.

4.1.4 Principe d'accessibilité organisationnelle

Le modèle d'analyse développé dans ce mémoire vise principalement les petites et moyennes entreprises. Contrairement aux grandes organisations, celles-ci disposent rarement d'équipes spécialisées en sécurité ou de ressources dédiées à la gestion de la sécurité organisationnelle.

Dans de nombreux cas, les décisions relatives à la sécurité sont prises par des gestionnaires dont la formation principale ne relève pas du domaine de la sécurité. Cette réalité impose une contrainte importante dans la conception d'un outil d'analyse. L'architecture retenue doit permettre une compréhension rapide des résultats et faciliter la prise de décision sans nécessiter une expertise technique approfondie.

L'objectif de l'outil n'est pas de remplacer une analyse professionnelle complète, mais de fournir un instrument d'aide à la décision permettant aux dirigeants de mieux comprendre la posture de sécurité de leur organisation et d'identifier les priorités d'amélioration.

4.1.5 Principe de lisibilité décisionnelle

Un outil d'analyse destiné aux organisations ne disposant pas d'expertise spécialisée doit offrir une représentation claire et synthétique des résultats.

Une architecture trop complexe ou reposant sur un nombre excessif de catégories analytiques risque de nuire à l'interprétation des résultats et à l'utilité stratégique de l'outil. À l'inverse, une structure trop simplifiée pourrait masquer des éléments importants du dispositif de protection.

L'architecture proposée vise donc à atteindre un équilibre entre rigueur conceptuelle et lisibilité décisionnelle. Elle repose sur un nombre limité de catégories analytiques permettant une lecture rapide de la posture de sécurité tout en conservant une capacité d'analyse pertinente.

4.1.6 Principe de stabilité structurelle et d'adaptabilité opérationnelle

La sécurité organisationnelle évolue constamment sous l'effet des transformations technologiques, de l'émergence de nouvelles menaces et de l'évolution des pratiques organisationnelles. Dans ce contexte, une architecture d'analyse reposant sur une liste figée de contrôles de sécurité risquerait de devenir rapidement obsolète.

Le modèle proposé repose donc sur une distinction entre stabilité structurelle et adaptabilité opérationnelle. La stabilité structurelle concerne les catégories analytiques utilisées pour organiser les mécanismes de protection. Ces catégories doivent être suffisamment générales pour demeurer pertinentes malgré l'évolution des technologies et des menaces.

À l'inverse, l'adaptabilité opérationnelle concerne les mécanismes concrets de protection déployés par l'organisation. Ceux-ci peuvent évoluer ou être remplacés sans remettre en question la structure analytique du modèle.

Cette distinction permet d'intégrer de nouveaux mécanismes de sécurité dans l'architecture d'analyse sans nécessiter une modification de sa structure fondamentale.

4.2 Architecture conceptuelle du modèle d'analyse

Les principes directeurs présentés dans la section précédente établissent les fondements conceptuels ayant guidé la conception de l'outil d'analyse de la posture de sécurité globale. La présente section expose l'architecture analytique résultant de la démarche de structuration conceptuelle décrite au chapitre 3.

Cette architecture vise à organiser les mécanismes de protection d'une organisation selon une structure permettant d'en faciliter l'analyse systémique. Plutôt que de considérer les contrôles de sécurité comme une accumulation de mesures indépendantes, le modèle proposé cherche à structurer ces mécanismes en fonction de leur rôle dans la protection des actifs organisationnels ainsi que de la nature des moyens mobilisés pour assurer cette protection.

L'architecture retenue repose sur le croisement de deux dimensions analytiques complémentaires. La première concerne les fonctions fondamentales de la sécurité, soit empêcher, détecter, retarder et répondre. La seconde concerne les familles de contrôles de sécurité, soit les technologies, équipements et services, les procédures ainsi que le facteur humain.

Le croisement de ces deux dimensions permet de structurer l'analyse de la posture de sécurité sous la forme d'une matrice analytique composée de douze catégories. Cette structure vise à offrir une représentation synthétique et accessible du dispositif de sécurité d'une organisation afin de faciliter l'identification des déséquilibres et des lacunes systémiques.

4.2.1 Les fonctions fondamentales des contrôles de sécurité

Dans plusieurs disciplines de la sécurité, les mécanismes de protection peuvent être analysés selon la fonction qu'ils remplissent dans la gestion d'un événement susceptible de compromettre un actif organisationnel. Toutefois, la manière de catégoriser ces fonctions varie selon les domaines professionnels.

Dans le domaine du filtrage de sécurité des personnes, la notion de fonctions de contrôle est relativement peu utilisée. Les pratiques professionnelles reposent davantage sur des processus d'enquête et d'évaluation visant à déterminer si une personne présente un niveau de fiabilité compatible avec l'accès à certains actifs sensibles. Ces processus incluent notamment la vérification des antécédents, l'analyse du parcours professionnel, les entrevues de sécurité et l'évaluation de facteurs de vulnérabilité. La logique dominante dans ce domaine n'est donc pas une catégorisation fonctionnelle des mécanismes de protection, mais plutôt une démarche d'enquête visant à réduire le risque associé à l'accès d'un individu à un actif organisationnel.

En sécurité physique, la littérature et les pratiques professionnelles reposent généralement sur une séquence fonctionnelle bien établie comprenant les fonctions de contrôle de la sécurité suivantes :

- décourager
- empêcher
- détecter
- retarder
- répondre

Ces fonctions décrivent les différentes étapes par lesquelles un dispositif de sécurité peut intervenir afin d'empêcher la compromission d'un actif. La fonction de réponse ne doit pas être interprétée comme une intervention survenant uniquement après un incident. Dans le domaine de la sécurité physique, elle correspond plutôt à l'ensemble des actions permettant d'intervenir avant que l'actif ne soit compromis.

Par exemple, dans un contexte de sécurité incendie, l'intervention rapide des services d'urgence sur un feu de poubelle à proximité d'un bâtiment constitue une réponse visant à empêcher la propagation de l'incendie et la destruction de l'édifice. Cette logique d'intervention s'inscrit dans la chaîne de protection des actifs et ne relève pas des mécanismes de continuité des activités.

Il importe donc de distinguer cette fonction de réponse des mécanismes relevant des plans de contingence organisationnels, tels que les plans de continuité des activités (BCP - Business Continuity Planning) ou les plans de reprise des activités ou des systèmes (DRP - Disaster Recovery Planning). Ces derniers interviennent généralement après la compromission d'un actif ou après une interruption majeure des opérations.

De manière comparable, dans le domaine de la cybersécurité, les fonctions des contrôles de sécurité sont généralement décrites mais à l'aide d'une terminologie légèrement différente. Les cadres de référence distinguent souvent les catégories suivantes :

- contrôles dissuasifs
- contrôles préventifs
- contrôles détectifs
- contrôles correctifs
- contrôles compensatoires
- contrôles de recouvrement

Ces catégories correspondent globalement aux mêmes logiques d'intervention que celles observées en sécurité physique, mais elles introduisent certaines distinctions supplémentaires.

Les contrôles compensatoires correspondent à des mécanismes alternatifs permettant d'atteindre un niveau de sécurité équivalent lorsqu'un contrôle préventif ne peut être appliqué tel quel. Par exemple, une organisation peut exiger l'authentification biométrique pour accéder à un système informatique. Toutefois, si un utilisateur est incapable d'utiliser ce mécanisme pour des raisons physiques, un contrôle compensatoire doit être mis en place afin de maintenir un niveau de sécurité équivalent.

Les contrôles correctifs, quant à eux, correspondent aux mesures mises en œuvre après la détection d'une activité malveillante afin de limiter la progression de l'incident ou de restaurer l'intégrité d'un système. Conceptuellement, cette fonction correspond largement à ce qui est désigné comme la fonction de réponse dans le domaine de la sécurité physique.

Enfin, les contrôles de recouvrement regroupent les mécanismes permettant de restaurer les systèmes ou les données après un incident majeur. Ces mesures s'inscrivent généralement dans le cadre des plans de continuité des activités ou des plans de reprise après sinistre.

L'analyse comparative de ces deux cadres fonctionnels met en évidence plusieurs différences. Premièrement, la cybersécurité distingue explicitement certaines catégories, comme les contrôles compensatoires ou correctifs, qui correspondent en réalité à des variantes

fonctionnelles de mécanismes déjà présents dans d'autres domaines. Deuxièmement, le domaine cyber ne comporte généralement pas de catégorie fonctionnelle explicitement dédiée au retardement d'une menace, bien que plusieurs mécanismes puissent produire cet effet. Par exemple, le verrouillage temporaire d'un compte après un nombre excessif de tentatives d'authentification constitue une mesure qui ralentit la progression d'une attaque sans être explicitement catégorisée comme telle.

Troisièmement, les classifications utilisées en cybersécurité intègrent souvent des mécanismes relevant directement des plans de contingence organisationnels, notamment les contrôles de recouvrement liés à la restauration des systèmes et des données.

Dans le cadre du présent projet de recherche, il a été décidé de retenir une structure fonctionnelle inspirée du domaine de la sécurité physique, conformément aux principes directeurs exposés à la section 4.1. Ce choix repose notamment sur la nature des termes utilisés dans cette structure fonctionnelle. Contrairement à plusieurs classifications utilisées dans d'autres domaines de la sécurité, qui reposent principalement sur des adjectifs décrivant des catégories de contrôles (préventif, détectif, correctif, etc.), l'approche issue de la sécurité physique privilégie l'utilisation de verbes d'action décrivant les fonctions opérationnelles du dispositif de sécurité (empêcher, détecter, retarder, répondre). Cette formulation met davantage l'accent sur la dimension active de la sécurité, en décrivant les actions qu'un système de protection doit être en mesure d'exécuter pour prévenir la compromission d'un actif.

Par ailleurs, le domaine de la sécurité physique constitue historiquement l'un des fondements des pratiques modernes de gestion de la sécurité. Plusieurs concepts aujourd'hui utilisés dans les domaines de la cybersécurité et de la sécurité de l'information trouvent leur origine dans les approches développées dans ce domaine. Or, dans la littérature contemporaine, les classifications issues de la cybersécurité tendent à être largement reprises dans l'ensemble des disciplines de la sécurité. Dans le cadre de ce travail, il a été jugé pertinent de s'appuyer sur la terminologie fonctionnelle issue de la sécurité physique afin de préserver cette logique d'intervention active dans l'analyse des mécanismes de protection.

La Figure 4.1 présente le positionnement temporel des principales fonctions de sécurité physique et de cybersécurité ainsi que leur relation avec les mécanismes de continuité et de reprise des affaires. Cette représentation illustre notamment que les fonctions empêcher, détecter, retarder et répondre interviennent à différents moments dans la chronologie d'un incident et ne doivent pas être confondues avec les mécanismes de récupération et de continuité organisationnelle.

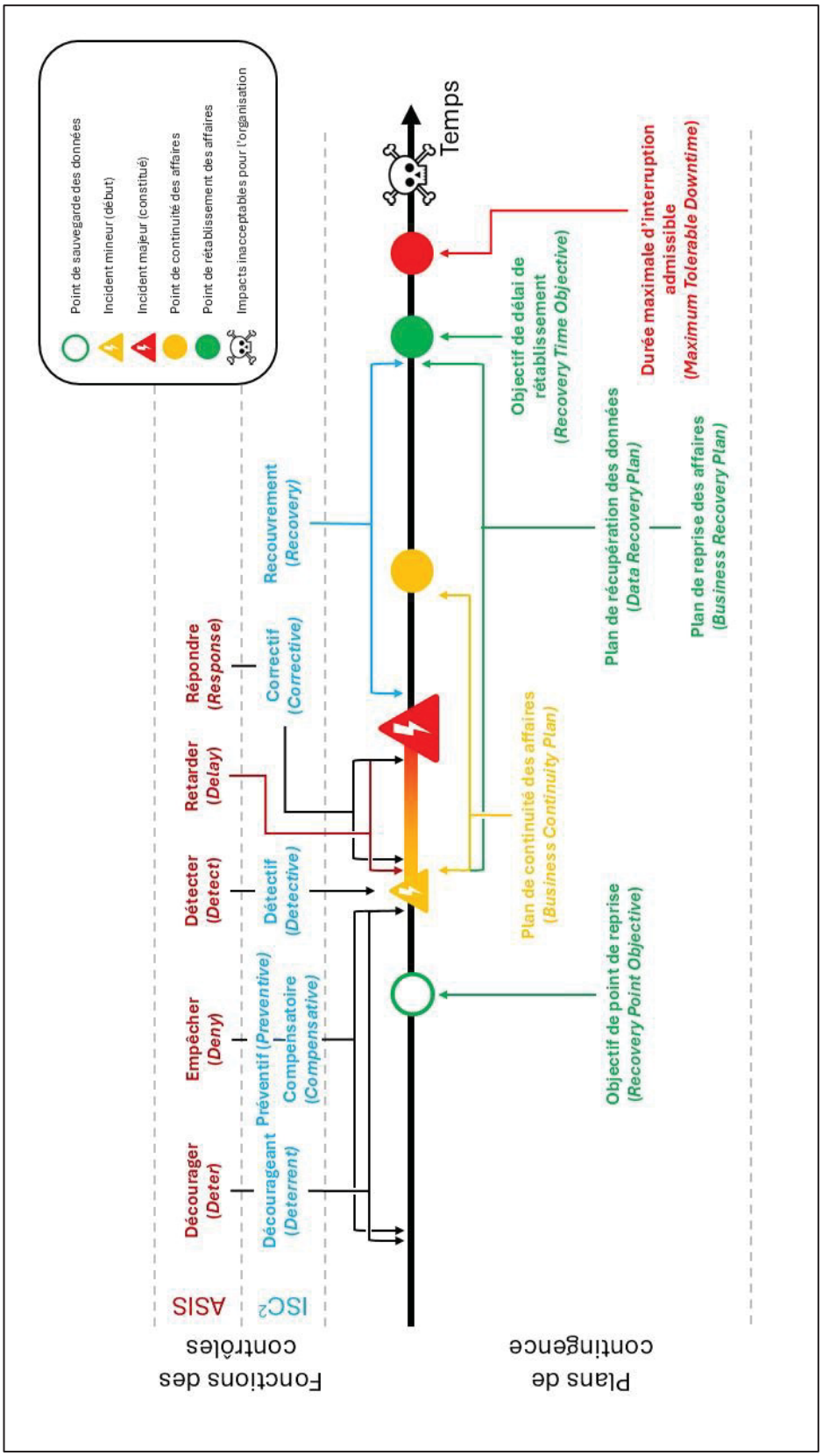


Figure 4.1 Positionnement des fonctions de sécurité physique, cybernétique et des plans de contingence dans la chronologie d'un incident

Toutefois, une adaptation a été apportée à ce modèle afin de permettre son application dans une perspective véritablement holistique de la sécurité organisationnelle. Plus précisément, la fonction décourager n'a pas été retenue comme catégorie fonctionnelle distincte. Les mécanismes visant à décourager une attaque reposent essentiellement sur l'influence du comportement d'un acteur humain et s'adressent donc principalement à des menaces intentionnelles, dites menaces « pensantes ». Or, plusieurs événements susceptibles d'affecter un actif organisationnel ne relèvent pas de ce type de menace. Les événements météorologiques, les incendies accidentels ou certaines défaillances techniques constituent des menaces dites « non pensantes » pour lesquelles la notion de dissuasion n'est pas applicable.

Dans une perspective d'analyse globale des dispositifs de sécurité, il apparaît donc préférable d'intégrer les mécanismes de dissuasion dans la fonction empêcher, puisqu'ils contribuent également à empêcher le passage à l'acte ou l'accès à un actif protégé. L'augmentation des inhibitions ou de la perception du risque peut en effet contribuer à empêcher une action malveillante, tout en participant à signaler qu'un système ou un site est protégé et contrôlé.

Sur cette base, l'architecture d'analyse développée dans ce mémoire retient quatre fonctions fondamentales de la sécurité :

- empêcher
- détecter
- retarder
- répondre

Ces fonctions permettent de structurer l'analyse des mécanismes de protection selon leur rôle dans la prévention de la compromission d'un actif organisationnel.

La fonction empêcher constitue généralement le premier niveau de protection d'un système de sécurité. Elle correspond le plus souvent aux mécanismes situés au périmètre d'un système, d'un site ou d'une ressource. L'objectif n'est pas nécessairement d'empêcher de manière absolue toute tentative d'accès, mais plutôt d'établir un premier niveau de contrôle démontrant

que le système ou le site est sécurisé et surveillé. Il peut s'agir, par exemple, d'un poste informatique nécessitant un mot de passe pour être utilisé, d'une porte extérieure d'édifice verrouillée ou d'un dispositif de contrôle d'accès limitant l'entrée à certaines zones. Les mécanismes visant à décourager une tentative d'intrusion peuvent également être intégrés à cette fonction dans la mesure où ils contribuent à empêcher le passage à l'acte.

La fonction détecter correspond au moment où un événement anormal est identifié par le dispositif de sécurité. Elle constitue le point central à partir duquel le système de sécurité peut déclencher une intervention appropriée. Pour être efficace, la détection repose généralement sur deux éléments complémentaires : une détection primaire et un mécanisme de validation. La détection primaire vise à identifier le plus rapidement possible qu'un événement inhabituel est en cours. La validation permet quant à elle de confirmer la nature de l'événement détecté afin de déterminer la réponse appropriée et de s'assurer que l'unité d'intervention disposera de la capacité nécessaire pour faire face à la menace. Par exemple, le déclenchement d'une station manuelle d'alarme incendie constitue un mécanisme de détection primaire. L'utilisation d'un système de caméras de surveillance peut ensuite permettre de valider la nature de l'événement observé. L'événement détecté pourrait correspondre à un incendie réel, à une personne blessée nécessitant une assistance ou encore à une situation de violence active.

La fonction retarder regroupe les mécanismes visant à ralentir la progression d'un événement en cours afin de permettre une réponse appropriée. Dans la pratique, les mécanismes de retardement correspondent, dans la quasi-totalité des cas, aux mêmes contrôles que ceux utilisés dans la fonction empêcher. La différence ne réside donc pas principalement dans la nature des contrôles utilisés, mais dans le moment où ils interviennent dans la séquence de l'incident. Les mécanismes associés à la fonction empêcher sont déployés en amont afin de constituer un premier niveau de protection, alors que les mécanismes associés à la fonction retarder interviennent temporellement après qu'il y ait eu détection d'un événement, dans le but de ralentir sa progression et de permettre le déploiement d'une réponse appropriée. Par exemple, un ordinateur protégé par un mot de passe constitue un mécanisme visant à empêcher un accès non autorisé. Toutefois, si ce même système verrouille automatiquement une session

après la détection d'une activité suspecte, ce mécanisme contribue alors à retarder la progression de l'événement afin de permettre une intervention.

Enfin, la fonction répondre correspond aux mécanismes permettant d'intervenir sur un événement en cours avant que la compromission complète de l'actif ne se produise. Il ne s'agit donc pas d'interventions relevant des plans de contingence organisationnels, mais bien d'actions visant à contenir ou neutraliser la menace. L'efficacité de cette fonction repose principalement sur deux éléments : le temps de réponse et la capacité d'endiguement de l'unité d'intervention. Une intervention rapide ne constitue pas en soi une réponse efficace si l'unité déployée ne possède pas les compétences, l'équipement ou l'autorité nécessaires pour faire face à la menace. Par exemple, déployer rapidement un agent de sécurité non armé lors d'un événement impliquant un tireur actif dans une installation industrielle ne constitue pas nécessairement une réponse efficace si cet agent ne possède ni la formation ni les moyens nécessaires pour intervenir face à une menace armée. Dans une telle situation, l'absence de capacité d'endiguement peut transformer l'intervenant en victime supplémentaire plutôt qu'en solution opérationnelle.

Ces quatre fonctions structurent ainsi l'analyse des mécanismes de protection selon leur contribution à la prévention de la compromission des actifs organisationnels.

4.2.2 Familles de contrôles de sécurité

Comme l'a montré la section précédente, les contrôles de sécurité peuvent être classés selon la fonction qu'ils remplissent dans la gestion d'un événement susceptible de compromettre un actif organisationnel. Toutefois, dans plusieurs disciplines de la sécurité, les contrôles sont également classés selon la nature des moyens utilisés pour mettre en œuvre ces mécanismes de protection. Ces regroupements sont généralement désignés comme des familles de contrôles de sécurité.

Ainsi, les contrôles de sécurité peuvent être analysés selon deux logiques de classification complémentaires. La première consiste à les classer selon la fonction qu'ils remplissent dans la séquence d'un événement de sécurité. La seconde consiste à les classer selon la nature des moyens mobilisés pour mettre en œuvre ces mécanismes de protection. Ces deux approches ne s'opposent pas, mais permettent plutôt d'analyser les mêmes contrôles selon deux dimensions différentes.

Dans le domaine du filtrage de sécurité des personnes, cette classification est inexistante. Les pratiques professionnelles reposent plutôt sur des processus d'enquête et d'évaluation visant à déterminer le niveau de fiabilité d'un individu avant de lui accorder l'accès à certains actifs organisationnels. Ces processus incluent notamment la vérification des antécédents, l'analyse du parcours professionnel, les entrevues de sécurité et l'évaluation de facteurs de vulnérabilité. Dans ce domaine, l'objectif consiste principalement à réduire le risque associé à l'accès d'une personne à un actif sensible, plutôt qu'à déployer des mécanismes de protection appartenant à différentes familles de contrôles.

En sécurité physique, les mécanismes de protection sont généralement regroupés selon trois grandes composantes :

- mesures techniques ou systèmes électroniques
- mesures procédurales
- élément humain

Les mesures techniques ou systèmes électroniques regroupent les technologies utilisées pour surveiller un site, détecter des événements anormaux et transmettre l'information nécessaire à l'intervention. Cette catégorie inclut notamment les systèmes de contrôle d'accès, les systèmes de vidéosurveillance, les systèmes de détection d'intrusion ainsi que les systèmes de communication utilisés par les intervenants de sécurité.

Les mesures procédurales regroupent l'ensemble des règles et des processus organisationnels encadrant l'utilisation des dispositifs de sécurité. Elles incluent notamment les consignes de poste, les procédures d'opération standard, les plans d'urgence ou encore les protocoles d'intervention.

L'élément humain correspond aux personnes responsables d'observer les systèmes, d'interpréter les situations et d'intervenir physiquement afin de contenir ou neutraliser une menace. Cette composante inclut notamment les agents de sécurité, les forces d'intervention et les opérateurs de centres de surveillance.

Pour ce qui est du domaine de la cybersécurité, les contrôles de sécurité sont également classés selon trois grandes catégories :

- contrôles administratifs
- contrôles techniques
- contrôles physiques

Les contrôles administratifs regroupent les politiques, procédures, normes et mécanismes de gouvernance encadrant l'utilisation sécuritaire des systèmes d'information. Cette catégorie inclut notamment les politiques de sécurité, les programmes de formation et de sensibilisation, les procédures de gestion des incidents ou encore les processus de gestion des accès.

Les contrôles techniques, parfois appelés contrôles logiques, correspondent aux mécanismes matériels et logiciels utilisés pour protéger les systèmes informatiques et les données. Cette catégorie inclut notamment les pare-feu, les systèmes de détection d'intrusion informatique, les mécanismes de chiffrement ou les solutions d'authentification multi-facteurs.

Les contrôles physiques regroupent les mesures tangibles visant à protéger les infrastructures technologiques et les équipements contre les accès non autorisés ou les dommages matériels. Ces contrôles incluent notamment les serrures, les systèmes de contrôle d'accès, les caméras

de surveillance ou les systèmes de protection environnementale comme les dispositifs d'extinction incendie.

L'analyse comparative de ces classifications met en évidence une limite importante. Certaines structures introduisent directement des domaines de sécurité spécifiques dans la catégorisation des contrôles. Par exemple, la catégorie « contrôles physiques » utilisée dans plusieurs cadres de cybersécurité fait explicitement référence au domaine de la sécurité physique. Cette approche présente toutefois une limite conceptuelle, puisqu'elle mélange la nature des contrôles avec les domaines disciplinaires auxquels ils sont associés. Elle peut également laisser entendre que la sécurité physique constitue un domaine distinct des approches technologiques, alors qu'elle repose aujourd'hui sur des systèmes hautement techniques. Les systèmes contemporains de sécurité physique intègrent en effet de nombreuses technologies avancées, notamment la biométrie comportementale et physiologique, l'analyse vidéo assistée par intelligence artificielle, les mécanismes cryptographiques utilisés dans les systèmes de contrôle d'accès électroniques, ainsi que diverses infrastructures informatiques nécessaires à l'exploitation de ces dispositifs.

Dans le cadre du présent projet de recherche, l'objectif consiste plutôt à adopter une perspective holistique de la sécurité, permettant d'analyser simultanément plusieurs domaines de protection sans en privilégier un en particulier. Il apparaît donc préférable d'utiliser une classification reposant sur la nature des moyens mobilisés, plutôt que sur les domaines disciplinaires auxquels ces contrôles sont traditionnellement associés.

Sur cette base, l'architecture d'analyse développée dans ce mémoire retient trois familles de contrôles de sécurité :

- contrôles technologiques, équipements et services
- contrôles administratifs et procéduraux
- contrôles humains

La famille technologies, équipements et services regroupe les dispositifs matériels, technologiques ou les capacités opérationnelles mobilisées pour mettre en œuvre des mécanismes de sécurité. Cette catégorie inclut notamment les systèmes électroniques de sécurité, les dispositifs physiques de protection, les équipements informatiques de protection ainsi que certains services contribuant directement aux opérations de sécurité.

L'intégration de la notion de services dans cette catégorie vise à résoudre un dilemme conceptuel observé dans plusieurs classifications traditionnelles des contrôles de sécurité. En effet, certaines mesures de protection reposent sur l'intervention de ressources humaines spécialisées, telles que les agents de sécurité, les services policiers ou les services incendie. Dans la pratique, ces ressources sont généralement considérées comme des capacités opérationnelles du système de protection, au même titre que certains équipements ou technologies. Par exemple, l'intégration d'un service de sécurité contractuel, d'un centre de télésurveillance ou encore de la capacité d'intervention d'un service incendie constitue un élément structurant du dispositif de sécurité d'un site.

Il apparaît également pertinent de distinguer ces ressources des contrôles appartenant à la famille des contrôles humains. Dans la majorité des situations, l'organisation analysée ne contrôle pas directement la formation, la sensibilisation ou les pratiques professionnelles de ces intervenants, qui sont fréquemment fournis par des organisations externes. Les mécanismes de sensibilisation et de formation relèvent donc davantage de la gestion interne du personnel de l'organisation que des capacités d'intervention associées à ces services. Afin de maintenir une cohérence méthodologique dans la classification proposée, les services de sécurité et d'intervention, qu'ils soient fournis par des ressources externes ou internes à l'organisation, sont donc regroupés dans la famille des contrôles technologiques, équipements et services.

La famille administratifs et procéduraux regroupe les règles, politiques, procédures et processus organisationnels encadrant la mise en œuvre des mesures de sécurité. Cette catégorie inclut notamment les politiques de sécurité, les procédures d'intervention en cas d'incident, les protocoles de gestion des accès ou les plans d'urgence.

La famille des contrôles humains regroupe les mécanismes visant principalement à influencer le comportement des individus participant aux activités de l'organisation. Cette catégorie inclut notamment les activités de sensibilisation, les programmes de formation et les initiatives visant à développer une culture organisationnelle favorable à la sécurité.

Bien que ces mécanismes soient généralement associés aux employés de l'organisation, ils peuvent également s'étendre aux autres personnes interagissant avec les actifs protégés, notamment les visiteurs, les clients ou les utilisateurs d'un site. Dans ce contexte, les mesures relevant de cette famille peuvent inclure, par exemple, l'affichage de consignes de sécurité, les campagnes de sensibilisation destinées aux usagers ou encore les dispositifs visant à orienter les comportements de manière sécuritaire dans un environnement donné.

Ces trois familles de contrôles constituent ainsi le second axe d'analyse de l'outil développé dans ce mémoire, permettant d'évaluer les mécanismes de protection non seulement selon la fonction qu'ils remplissent dans la gestion d'un événement de sécurité, mais également selon la nature des moyens mobilisés pour assurer ces fonctions.

4.2.3 Choix de la structure analytique croisée

Les deux sous-sections précédentes ont permis d'établir les deux axes de classification retenus dans le cadre de ce mémoire. D'une part, les contrôles de sécurité peuvent être classés selon leur fonction dans la protection d'un actif organisationnel, soit empêcher, détecter, retarder ou répondre. D'autre part, ces mêmes contrôles peuvent être classés selon leur famille, c'est-à-dire selon la nature des moyens mobilisés pour mettre en œuvre cette protection, soit les contrôles technologiques, équipements et services, les contrôles administratifs et procéduraux, ainsi que les contrôles humains.

L’enjeu de la présente section n’est donc pas de mettre en relation des objets distincts, mais de déterminer la manière la plus cohérente de représenter simultanément deux axes de classification portant sur les mêmes contrôles de sécurité.

Plusieurs modes de représentation pouvaient être envisagés. Une première possibilité aurait consisté à présenter séparément les fonctions de contrôle et les familles de contrôle, sous la forme de deux listes ou de deux grilles indépendantes. Une telle approche aurait toutefois eu pour effet de dissocier deux dimensions qui doivent être examinées conjointement pour apprécier la posture de sécurité d’une organisation. En effet, un contrôle de sécurité ne se comprend pleinement que lorsqu’il est possible d’identifier à la fois ce qu’il fait dans la dynamique de protection d’un actif et la nature du moyen mobilisé pour produire cet effet.

Une deuxième possibilité aurait consisté à adopter une structure beaucoup plus détaillée intégrant explicitement, dès le niveau principal de représentation, les différents domaines de la sécurité, tels que la sécurité physique, la cybersécurité et le filtrage de sécurité des personnes. Une telle structure aurait toutefois alourdi considérablement l’outil et nui à sa lisibilité. Elle aurait aussi compliqué sa reproduction dans des formats courants de communication organisationnelle, tels qu’un document imprimé, un rapport synthèse ou une présentation PowerPoint.

Le choix retenu dans ce mémoire consiste donc à utiliser une structure analytique bidimensionnelle fondée sur le croisement des fonctions de contrôle et des familles de contrôle. Cette structure permet de représenter simultanément les deux axes de classification retenus tout en conservant un niveau de simplicité compatible avec les principes d’accessibilité organisationnelle et de lisibilité décisionnelle exposés à la section 4.1.

Concrètement, cette structure prend la forme d’une grille de lecture comprenant quatre lignes correspondant aux fonctions de contrôle et trois colonnes correspondant aux familles de contrôle. Le croisement de ces deux axes produit douze catégories analytiques. Les contrôles observés au sein d’une organisation peuvent être classés dans ces catégories. La grille ne

présente toutefois pas directement ces contrôles de manière détaillée. Elle en offre plutôt une représentation qualitative synthétique, fondée sur le niveau relatif de présence des contrôles dans chacune des cellules. Le Tableau 4.1 illustre cette structure analytique générale.

Tableau 4.1 Structure analytique générale fondée sur le croisement des fonctions et des familles de contrôles de sécurité

Familles / Fonctions	Technologies, équipements et services	Administratifs et procéduraux	Humains
Empêcher			
Détecter			
Retarder			
Répondre			

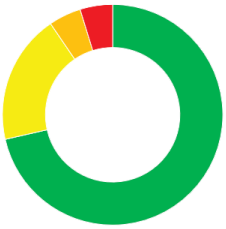
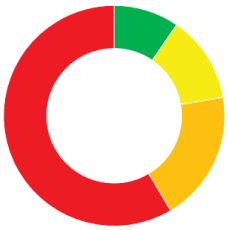
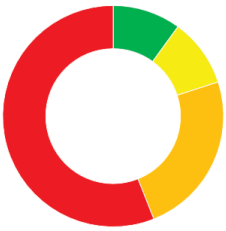
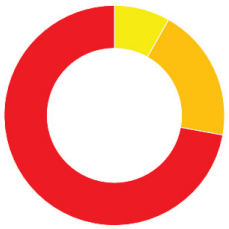
Afin de rendre cette structure exploitable dans un contexte organisationnel, un mode de représentation qualitative des contrôles a été défini.

Chaque contrôle est évalué selon une échelle ordinale allant de 0 à 3. La cote 3 correspond à un contrôle pleinement implanté et efficace, la cote 2 à un contrôle partiellement implanté, la cote 1 à un contrôle faiblement implanté, et la cote 0 à l'absence de contrôle ou à une

implantation inadéquate. La mention n.a. est utilisée lorsque le contrôle n'est pas applicable dans le contexte analysé et n'est pas prise en compte dans les calculs.

Les résultats agrégés de cette évaluation sont ensuite représentés visuellement dans chacune des cellules de la grille. Chaque cellule contient un graphique circulaire en forme de beigne illustrant la distribution relative des contrôles selon leur niveau d'implantation. La portion verte représente les contrôles cotés à 3, la portion orange ceux cotés à 2, la portion jaune ceux cotés à 1 et la portion rouge ceux cotés à 0. Le Tableau 4.2 illustre cette intégration du mécanisme de représentation au sein de la structure analytique (exemple avec des données simulées).

Tableau 4.2 Représentation qualitative de la posture de sécurité dans la structure analytique 4 x 3

Familles / Fonctions	Technologies, équipements et services	Administratifs et procéduraux	Humains
Empêcher			
Détecter			
Retarder			
Répondre			

Cette représentation ne montre donc pas les contrôles individuellement, mais la répartition qualitative des résultats obtenus pour l'ensemble des contrôles associés à chaque cellule. Elle

permet de conserver une lecture synthétique de la posture de sécurité tout en offrant une information plus nuancée que la simple présence ou absence de contrôles.

Le choix de cette structure ne signifie toutefois pas que les différents domaines de la sécurité sont fusionnés indistinctement dans l'analyse. En pratique, les contrôles issus de la sécurité physique, de la cybersécurité et du filtrage de sécurité peuvent être traités séparément lorsque la précision analytique l'exige. La structure retenue vise plutôt à fournir un cadre commun de classification et un mode commun de représentation visuelle. Ainsi, des contrôles provenant de domaines distincts peuvent être affichés dans une même représentation synthétique de niveau supérieur, tout en conservant la possibilité d'être ventilés dans des analyses distinctes au besoin.

Cette précision est importante, car les domaines de la sécurité ne disparaissent pas dans l'architecture proposée. Ils se retrouvent à l'intérieur même des contrôles classés dans les différentes catégories analytiques. Ainsi, une même cellule peut regrouper des contrôles issus de la sécurité physique, de la cybersécurité ou du filtrage de sécurité. Il aurait donc été théoriquement possible de concevoir une représentation tridimensionnelle croisant les fonctions, les familles et les domaines. Toutefois, une telle représentation aurait été beaucoup plus difficile à utiliser, à imprimer, à projeter et à interpréter dans un contexte organisationnel.

La structure bidimensionnelle retenue constitue donc un compromis méthodologique entre richesse analytique et simplicité de représentation. Elle permet de conserver une architecture stable, même si les contrôles évoluent dans le temps, sont remplacés ou se transforment sous l'effet des changements technologiques ou organisationnels. Ce ne sont pas les catégories analytiques qui changent, mais les contrôles qui y sont classés.

Ce choix s'inscrit directement dans les principes directeurs exposés à la section 4.1. D'abord, il favorise l'intégration interdisciplinaire en retenant un cadre commun applicable à plusieurs domaines de la sécurité. Ensuite, il soutient le principe d'équilibre systémique en facilitant l'identification visuelle des zones fortement couvertes, des zones faiblement couvertes et des

déséquilibres généraux entre les fonctions et les familles de contrôle. Il respecte également le principe de cohérence fonctionnelle, puisqu'il oblige à examiner les contrôles selon le rôle qu'ils jouent dans la dynamique de protection des actifs. Enfin, il répond aux exigences d'accessibilité organisationnelle et de lisibilité décisionnelle en proposant une structure simple, reproductible et compréhensible pour des gestionnaires non spécialistes.

Il convient toutefois de souligner que cette structure n'a pas pour fonction de démontrer à elle seule qu'un dispositif de sécurité est adéquat ou pleinement efficace. Sa fonction première est plutôt de mettre en évidence les déséquilibres et les zones problématiques. Ainsi, la présence d'une cellule faiblement couverte ou vide constitue un indicateur clair d'une faiblesse potentielle du dispositif analysé. À l'inverse, une représentation visuellement homogène ou fortement remplie ne permet pas, à elle seule, de conclure que la posture de sécurité est satisfaisante.

C'est pourquoi la structure retenue doit pouvoir être déclinée à plusieurs niveaux. Une représentation générale peut d'abord regrouper l'ensemble des contrôles observés dans l'organisation. Cette représentation peut ensuite être ventilée par domaine de sécurité, par exemple en une représentation distincte pour la sécurité physique, une autre pour la cybersécurité et une autre pour le filtrage de sécurité des personnes. À son tour, chacune de ces représentations peut être subdivisée selon les événements indésirables considérés. La Figure 4.2 illustre cette logique de décomposition de la matrice globale en sous-matrices analytiques.

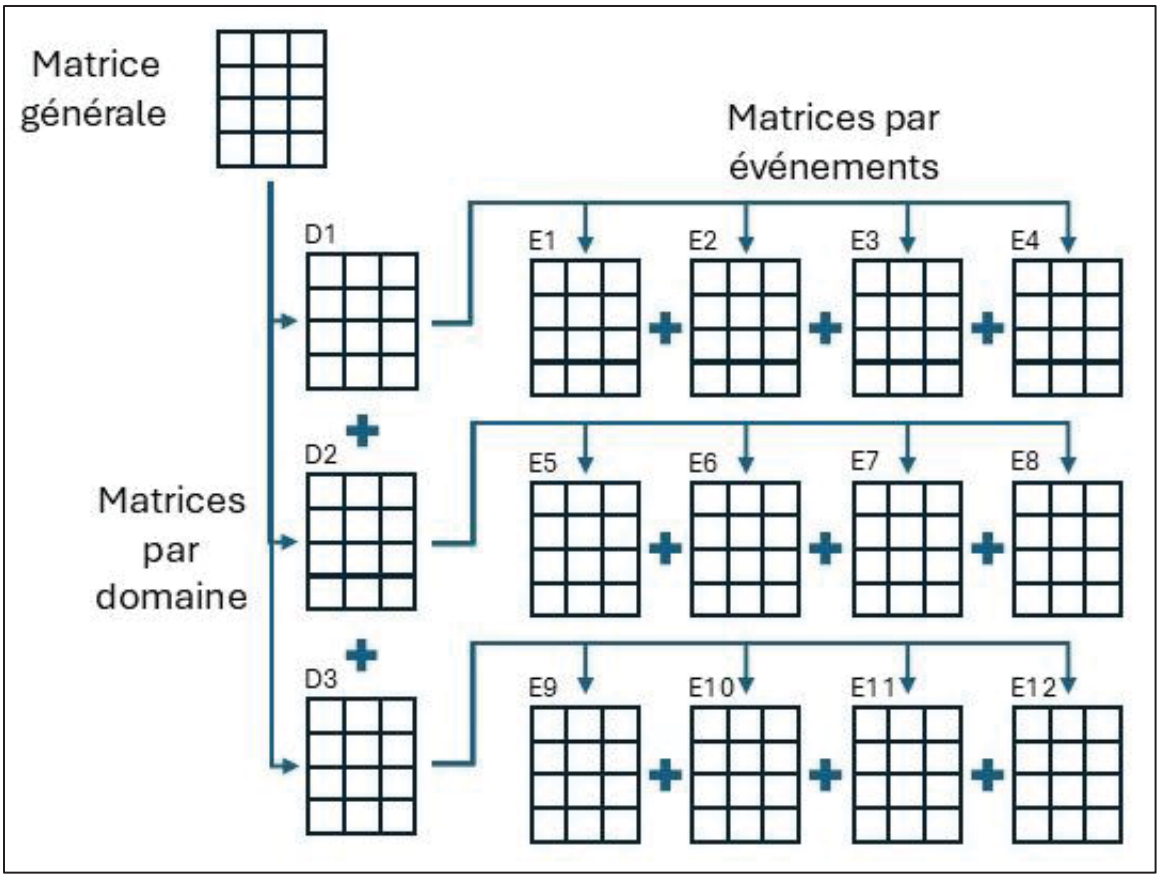


Figure 4.2 Logique de déclinaison analytique, de la matrice globale vers les matrices par domaine, puis vers les matrices associées aux événements d'exception

Cette capacité de déclinaison est essentielle à la valeur analytique de l'outil. Une représentation générale peut révéler un manque évident d'homogénéité, ce qui indique clairement un problème. En revanche, une représentation générale visuellement équilibrée doit être interprétée avec prudence. Elle peut simplement signifier qu'à un niveau agrégé, les contrôles semblent répartis de manière relativement homogène. Toutefois, cette apparente homogénéité peut résulter de la superposition de déséquilibres inverses présents dans des sous-ensembles distincts.

4.3 Fonctionnement de l'outil d'analyse

La structure analytique présentée à la section précédente constitue le support de représentation de la posture de sécurité. Son utilisation repose sur une démarche structurée permettant d'analyser, de manière concrète et opérationnelle, la capacité d'une organisation à faire face à différentes situations de sécurité.

Cette démarche s'articule autour de quatre étapes principales : la définition des événements indésirables, l'association des contrôles de sécurité, l'évaluation de leur niveau d'implantation et la compilation des résultats dans une matrice de représentation.

Il est important de préciser que ces quatre étapes font partie intégrante de la méthode développée dans le cadre de ce mémoire. Toutefois, pour des raisons liées à la propriété intellectuelle et à l'exploitation de l'outil, les éléments détaillés associés aux trois premières étapes ne sont pas présentés de manière exhaustive.

En effet, la sélection des événements indésirables repose sur une structuration globale couvrant plusieurs domaines de la sécurité, ce qui constitue un élément central de la méthode. De la même manière, l'association des contrôles de sécurité et leur caractérisation ont fait l'objet d'un travail structuré en amont, incluant leur classification selon les fonctions de sécurité, leur famille de contrôle ainsi que leur source, qu'elle soit issue de normes existantes ou de développements propriétaires.

L'étape d'évaluation repose quant à elle sur un ensemble de questions construites de manière à réduire la subjectivité et à obtenir une valeur standardisée. Ces questions ne sont pas détaillées dans ce mémoire pour des raisons de confidentialité.

La contribution explicitement documentée dans ce mémoire concerne la quatrième étape, soit la structuration, l'agrégation et la représentation des résultats, qui constitue le cœur de l'outil d'analyse proposé.

4.3.1 Sélection et définition des événements indésirables

Dans le cadre de cet outil, un événement indésirable est défini comme la combinaison d'un actif et d'une menace. Cette définition se distingue volontairement de celle du risque. Le risque correspondant à la combinaison d'une menace, d'un actif et d'un niveau de vulnérabilité résiduelle, alors que l'outil proposé se positionne en amont, en se concentrant sur les situations pouvant affecter un actif indépendamment du niveau de vulnérabilité. La méthode développée repose sur une sélection structurée d'événements indésirables couvrant plusieurs domaines de la sécurité, ce qui permet d'éviter une analyse fragmentée et de maintenir une vision globale.

À titre d'illustration, les événements indésirables peuvent être formulés de manière concrète en combinant explicitement un actif et une menace.

Exemples en sécurité physique

- Vol qualifié dans un site ouvert au public
- Violence au travail dans un environnement administratif
- Accès non autorisé forcé à une zone restreinte
- Accès non autorisé subreptice à un bâtiment
- Livraison d'un colis contenant un engin explosif à une réception
- Incendie volontaire dans un entrepôt
- Attaque de type tireur actif dans un espace public
- Impact volontaire d'un véhicule sur une entrée de bâtiment
- Surveillance active d'un site en préparation d'une attaque

Ces exemples illustrent des situations où des actifs physiques, des personnes ou des infrastructures sont ciblés par des menaces intentionnelles.

Exemples en cybersécurité

- Chiffrement des données d'un serveur de production par rançongiciel

- Perte de données à la suite d'une défaillance d'un disque dur
- Accès non autorisé à un système informatique
- Fuite de données causée par une mauvaise configuration
- Exfiltration d'information à partir d'un compte compromis
- Indisponibilité d'un service en ligne causée par une attaque par déni de service

Ces situations concernent directement des actifs informationnels et technologiques.

Exemples en filtrage de sécurité des personnes

- Espionnage d'une organisation par un employé
- Vente d'information sensible par un employé en difficulté financière
- Sabotage interne d'un système ou d'un processus
- Accès à un poste sensible par une personne non adéquatement filtrée
- Obtention d'un emploi à l'aide de fausses références

Ces événements mettent en évidence le rôle central du facteur humain dans la posture de sécurité.

Ces exemples illustrent la logique de construction des événements indésirables utilisée dans l'outil. Chaque événement est formulé de manière à être clair, observable et directement lié aux opérations de l'organisation.

Certains référentiels, notamment MITRE ATT&CK, proposent une association partielle entre des techniques d'attaque et des mesures de protection. Toutefois, ces approches demeurent généralement limitées à des menaces intentionnelles et ne permettent pas de structurer les contrôles de manière cohérente selon des fonctions de sécurité et des familles de moyens.

Les principaux cadres normatifs, tels que le NIST Cybersecurity Framework ou ISO/IEC 27001, proposent quant à eux des classifications fonctionnelles ou des catalogues de contrôles,

sans établir de lien explicite entre des événements indésirables spécifiques et les mécanismes de protection à mettre en œuvre.

En conséquence, il n'existe pas, à ce jour, de référentiel largement reconnu permettant d'associer de manière structurée des événements indésirables, définis comme la combinaison d'un actif et d'une menace, à un ensemble cohérent de contrôles de sécurité couvrant simultanément plusieurs domaines de la sécurité.

La liste exhaustive des événements indésirables utilisés dans l'outil n'est pas présentée dans ce mémoire, puisqu'elle constitue un élément propriétaire. Toutefois, la méthode de structuration présentée permet d'assurer une couverture cohérente et interdisciplinaire des différentes dimensions de la sécurité.

4.3.2 Association des contrôles de sécurité

À chaque événement indésirable est associé un ensemble de contrôles de sécurité visant à agir sur celui-ci.

Un même contrôle peut être applicable à plusieurs événements indésirables. Cette approche permet de refléter la réalité opérationnelle des organisations, où certaines mesures contribuent simultanément à la gestion de plusieurs situations. Par exemple, un mécanisme de gestion des accès peut contribuer à limiter un accès non autorisé, une fuite d'information ou un acte malveillant interne.

Contrairement à plusieurs approches où les contrôles sont présentés de manière isolée, la méthode développée repose sur une classification préalable des contrôles de sécurité. Cette classification constitue un élément central de l'outil.

En amont de l'utilisation par l'organisation, chaque contrôle a été caractérisé selon trois dimensions :

- Fonction de sécurité : empêcher, détecter, retarder ou répondre
- Famille de contrôle : technologies, équipements et services, administratifs et procéduraux ou humains
- Source du contrôle : issue de normes reconnues ou développement propriétaire

Les familles de contrôle utilisées correspondent exactement à celles définies dans la matrice présentée à la section 4.2, afin d'assurer une cohérence complète entre la collecte, l'analyse et la représentation des données.

Cette architecture des contrôles permet d'éviter un problème fréquent observé dans plusieurs méthodologies, où les contrôles sont traités en vrac, sans cohérence fonctionnelle ni interdépendance. Il en résulte souvent des postures de sécurité inefficace Cette classification des contrôles permet d'éviter un problème fréquent observé dans plusieurs méthodologies, où les contrôles sont traités en vrac, sans cohérence fonctionnelle ni interdépendance. Il en résulte souvent des postures de sécurité inefficaces.

À titre d'exemple :

- Capacité de détection sans capacité de réponse
- Présence de mesures technologiques sans encadrement administratif
- Déploiement d'équipements sans formation adéquate des utilisateurs

Dans ces situations, la présence de contrôles peut donner une impression de sécurité, sans pour autant permettre de gérer efficacement un événement indésirable.

L'approche proposée vise à corriger cette problématique en imposant une lecture structurée des contrôles à travers les fonctions de sécurité et les familles de contrôle. L'objectif n'est pas uniquement de vérifier la présence de contrôles, mais de s'assurer qu'ils contribuent de manière cohérente à la gestion complète d'un événement.

Les contrôles de sécurité utilisés dans l'outil proviennent de différentes sources issues de la sécurité physique, de la cybersécurité et du filtrage de sécurité des personnes. Ces sources incluent des normes reconnues, des guides techniques ainsi que des cadres de référence opérationnels.

En sécurité physique, des normes telles que celles développées par ASIS International, la National Fire Protection Association (notamment la norme NFPA 730), les standards de UL (UL 294) ou encore les normes CAN/ULC (CAN/ULC-S301) définissent de nombreux mécanismes de protection. Ces contrôles sont généralement bien définis sur le plan technique et opérationnel. Toutefois, ces référentiels ne proposent pas de classification systématique selon les fonctions de sécurité retenues dans ce mémoire, ni de structuration uniforme selon des familles de contrôles.

En cybersécurité, des cadres tels que la norme ISO/IEC 27001 et ISO/IEC 27002, le NIST (SP 800-53), les Center for Internet Security Critical Security Controls ou encore le cadre MITRE ATT&CK proposent des ensembles structurés de contrôles. Toutefois, ces contrôles sont généralement organisés selon des domaines ou des catégories administratives et techniques. Ils ne sont pas directement associés à des événements indésirables spécifiques et n'imposent pas une couverture fonctionnelle complète des mécanismes de protection.

Dans le domaine du filtrage de sécurité des personnes, les pratiques reposent notamment sur des cadres tels que la Norme sur le filtrage de sécurité du Gouvernement du Canada ou la Directive sur la sécurité du personnel du Treasury Board of Canada Secretariat. Ces approches sont structurées sous forme de processus d'enquête et d'évaluation, sans classification explicite en termes de fonctions de sécurité ou de familles de contrôles.

Ainsi, bien que les contrôles soient généralement bien définis individuellement dans ces différents référentiels, ils ne sont pas organisés de manière cohérente selon leur fonction dans la gestion d'un événement ni selon la nature des moyens mobilisés. L'approche proposée dans ce mémoire vise à combler cette lacune en introduisant une classification systématique des

contrôles, permettant leur association directe à des événements indésirables tout en assurant une couverture fonctionnelle et organisationnelle complète.

La liste exhaustive des contrôles, leur description détaillée ainsi que leur association précise avec les événements indésirables ne sont pas présentées dans ce mémoire, puisqu'elles constituent des éléments propriétaires de l'outil.

Toutefois, la logique d'association présentée permet de comprendre comment les contrôles s'inscrivent dans une architecture globale visant à couvrir de manière équilibrée l'ensemble des dimensions de la sécurité. Le Tableau 4.3, illustre cette architecture dans le cas où l'événement indésirable serait le vol d'un ordinateur sur le site.

Tableau 4.3 Liste de contrôles de sécurité illustrant une couverture cohérente pour l'événement indésirable « Vol d'un ordinateur sur le site »

Familles / Fonctions	Technologies, équipements et services	Administratifs et procéduraux	Humains
Empêcher	Contrôle d'accès électronique aux zones de bureaux (cartes, badges, lecteurs)	Politique de contrôle des accès limitant la présence aux zones de travail selon les rôles	Sensibilisation des employés aux bonnes pratiques de protection des équipements
Détecter	Système d'alarme intrusion en dehors des heures ouvrables	Procédure d'inventaire périodique des équipements informatiques	Vigilance des employés face à des comportements ou présences inhabituelles
Retarder	Dispositifs d'ancrage physique des ordinateurs (câbles antivol, stations verrouillées)	Procédure de sécurisation des postes de travail en fin de journée (rangement, verrouillage)	Interaction proactive avec une personne suspecte visant à créer un délai
Répondre	Intervention vocale à distance supportée par la vidéosurveillance	Procédure d'intervention immédiate en cas d'alarme ou de comportement suspect (ex. déplacement d'un agent, appel aux forces de l'ordre)	Intervention immédiate auprès d'une personne suspecte visant à interrompre la tentative de vol

Ce tableau illustre qu'un même type d'interaction, notamment dans la dimension humaine, peut relever de fonctions différentes selon l'intention opérationnelle. Une interaction visant à créer un délai relève de la fonction retarder, tandis qu'une intervention visant à interrompre l'action relève de la fonction répondre.

4.3.3 Évaluation du niveau d'implémentation des contrôles de sécurité

Une fois les événements indésirables définis et les contrôles de sécurité associés, l'étape suivante consiste à évaluer le niveau d'implémentation de ces contrôles au sein de l'organisation.

Cette étape vise à transformer une réalité opérationnelle en information structurée, afin d'alimenter la représentation de la posture de sécurité qui sera présentée à la section 4.4.

Dans le cadre de l'outil proposé, chaque contrôle de sécurité est évalué selon une échelle ordinale allant de 0 à 3, à laquelle s'ajoute la possibilité de désigner un contrôle comme non applicable (n.a.).

- 0 : contrôle absent ou inexistant
- 1 : contrôle faiblement implanté ou inefficace
- 2 : contrôle partiellement implanté ou appliqué de manière inconstante
- 3 : contrôle pleinement implanté et efficace
- n.a. : contrôle non applicable dans le contexte évalué

Cette échelle permet de capter de manière simple le niveau de maturité des mécanismes de protection, sans recourir à une évaluation quantitative complexe.

Toutefois, afin de limiter la subjectivité et de faciliter l'utilisation de l'outil dans des contextes organisationnels variés, notamment au sein de petites et moyennes entreprises, la collecte de l'information ne repose pas sur l'attribution directe d'une cote numérique par les répondants.

Chaque contrôle est plutôt évalué à l'aide d'énoncés descriptifs représentant différents niveaux d'implantation. Le répondant est invité à sélectionner l'énoncé qui correspond le mieux à sa réalité.

À titre d'exemple, pour un contrôle relatif à la robustesse d'un mot de passe :

- Mot de passe complexe respectant les meilleures pratiques (longueur élevée, diversité de caractères, absence de réutilisation)
- Mot de passe respectant certaines exigences minimales
- Mot de passe simple ou partiellement conforme
- Absence de mot de passe ou utilisation d'un mot de passe trivial

Chaque énoncé correspond implicitement à un niveau de l'échelle de 0 à 3, sans que cette correspondance soit explicitement visible pour le répondant.

Cette approche permet de réduire les biais liés à l'autoévaluation et d'améliorer la cohérence des réponses, tout en maintenant une simplicité d'utilisation adaptée à des utilisateurs non spécialisés en sécurité.

Une fois les réponses collectées, les niveaux d'implantation sont compilés et associés aux contrôles correspondants. Ces résultats constituent la base de la représentation visuelle de la posture de sécurité.

Il est important de noter qu'un même contrôle peut être associé à plusieurs événements indésirables. Dans ce cas, le contrôle est comptabilisé autant de fois qu'il est mobilisé, ce qui permet de refléter son importance relative dans la posture de sécurité globale.

Cette logique contribue à faire ressortir les contrôles structurants, c'est-à-dire ceux qui participent à la gestion de plusieurs événements, et qui jouent donc un rôle central dans le dispositif de sécurité.

Enfin, il convient de rappeler que cette étape d'évaluation ne vise pas à mesurer un niveau de risque au sens formel. Elle permet plutôt d'obtenir une appréciation structurée de l'état des contrôles de sécurité, qui sera ensuite interprétée à travers la matrice analytique.

L'objectif est de soutenir une lecture globale de la posture de sécurité, en mettant en évidence les déséquilibres, les lacunes et les concentrations de contrôles, plutôt que de produire une mesure chiffrée du risque.

4.3.4 Agrégation des résultats et représentation de la posture de sécurité

À l'issue de l'évaluation du niveau d'implémentation des contrôles de sécurité, les résultats obtenus sont agrégés afin de permettre leur intégration dans la structure analytique définie à la section 4.2. Cette étape constitue le point culminant de la méthode développée dans le cadre du présent mémoire, les étapes précédentes ayant pour objectif de produire une information structurée et exploitable permettant d'aboutir à une représentation cohérente de la posture de sécurité de l'organisation.

L'agrégation consiste à regrouper les contrôles évalués selon les deux axes de classification retenus, soit les fonctions de sécurité et les familles de contrôles. Chaque contrôle, préalablement caractérisé selon ces deux dimensions, est positionné dans l'une des douze cellules de la structure analytique, puis les résultats d'évaluation associés sont consolidés à l'intérieur de ces cellules. Cette consolidation ne vise pas à produire un indicateur numérique unique, mais à représenter la distribution qualitative des niveaux d'implémentation observés. Ainsi, pour chaque cellule, l'information correspond à la répartition des contrôles selon les différentes cotes d'évaluation, à l'exclusion des contrôles jugés non applicables. Cette

approche permet de conserver la richesse de l'information tout en évitant les simplifications excessives associées à l'utilisation d'indicateurs uniques.

Il convient également de souligner qu'un même contrôle peut être associé à plusieurs événements indésirables. Dans ce cas, il est comptabilisé pour chacun des événements auxquels il contribue, ce qui permet de refléter plus fidèlement la réalité opérationnelle et de faire ressortir les contrôles structurants du dispositif de sécurité, c'est-à-dire ceux qui interviennent dans plusieurs situations.

L'analyse des résultats agrégés doit être réalisée selon une logique progressive. Dans un premier temps, l'attention est portée sur la distribution des niveaux d'implémentation à l'échelle de l'ensemble de la structure analytique, afin d'identifier les déséquilibres potentiels entre les fonctions de sécurité et les familles de contrôles. Une distribution relativement uniforme des niveaux d'implémentation, même si elle se situe à un niveau intermédiaire, traduit généralement une cohérence dans la posture de sécurité, alors qu'une alternance marquée entre des niveaux élevés et des absences de contrôles met en évidence un déséquilibre structurel.

Dans cette perspective, l'acceptation d'un certain niveau de risque peut se traduire par la présence de contrôles moins développés, mais cette situation doit demeurer cohérente à l'échelle de l'ensemble de la structure. Une concentration de faiblesses dans une fonction ou une famille de contrôles en particulier constitue un indicateur plus préoccupant qu'une réduction uniforme du niveau de protection.

Si l'analyse met en évidence des déséquilibres ou soulève des interrogations, il est alors possible d'approfondir l'analyse en exploitant les données sous-jacentes. Cette démarche s'effectue de manière progressive, en passant d'abord d'une lecture globale à une analyse par domaine de la sécurité, notamment la sécurité physique, la cybersécurité ou le filtrage de sécurité des personnes, afin de préciser l'origine des déséquilibres observés. Si nécessaire, l'analyse peut être poursuivie à un niveau plus granulaire, en examinant les résultats associés

à des événements indésirables spécifiques, tel qu'illustré à Figure 4.2 Logique de déclinaison analytique, de la matrice globale vers les matrices par domaine, puis vers les matrices associées aux événements d'exception, présentée précédemment.

Ainsi, l'agrégation des résultats constitue un mécanisme structurant permettant d'organiser l'information issue de l'évaluation des contrôles de sécurité, tout en conservant la possibilité d'effectuer des analyses à différents niveaux de détail. Elle prépare la représentation de la posture de sécurité selon les modalités présentées à la section suivante.

4.4 Représentation graphique de la posture de sécurité

La section précédente a permis de définir la manière dont les résultats issus de l'évaluation des contrôles de sécurité sont agrégés et structurés au sein de la matrice analytique. Cette agrégation constitue la base de la représentation de la posture de sécurité de l'organisation.

Toutefois, afin de rendre cette information exploitable dans un contexte organisationnel, il est nécessaire de la traduire sous une forme visuelle permettant une lecture rapide et une compréhension intuitive des résultats. L'objectif n'est pas de présenter les contrôles individuellement, mais de proposer une représentation synthétique mettant en évidence la distribution des niveaux d'implémentation à travers les différentes fonctions de sécurité et familles de contrôles.

Dans cette perspective, une représentation graphique a été retenue afin de refléter de manière fidèle la structure analytique définie à la section 4.2, tout en facilitant son interprétation par des utilisateurs ne disposant pas nécessairement d'une expertise approfondie en sécurité. Les sous-sections suivantes présentent les objectifs de cette représentation, sa structure, ainsi que les principes guidant son interprétation.)

4.4.1 Objectifs de la représentation visuelle

La représentation visuelle de la posture de sécurité vise à offrir une lecture rapide, globale et cohérente des résultats issus de l'analyse, sans chercher à détailler individuellement l'ensemble des contrôles de sécurité. L'objectif est plutôt de fournir une synthèse permettant de comprendre, en un minimum de temps, l'état général des mesures de protection en place. Cette représentation doit permettre d'apprécier la cohérence du dispositif de sécurité en mettant en évidence la répartition des contrôles à travers les différentes fonctions de sécurité et familles de contrôles. Ainsi, en un coup d'œil, il devient possible d'identifier les zones présentant une couverture équilibrée, de même que celles où des déséquilibres structurels sont présents, notamment lorsqu'une fonction ou une famille de contrôles est sous-représentée par rapport aux autres.

Cette approche permet de dépasser une lecture fondée uniquement sur la quantité de contrôles pour se concentrer sur leur distribution et leur complémentarité. Elle vise également à faire ressortir les forces et les faiblesses globales de la posture de sécurité, en facilitant l'identification des zones où les contrôles sont bien implantés et de celles où des lacunes persistent. Par ailleurs, la représentation est conçue de manière à être accessible à des utilisateurs ne disposant pas nécessairement d'une expertise approfondie en sécurité, notamment dans un contexte de petites et moyennes entreprises, tout en conservant une base analytique rigoureuse. Enfin, elle constitue un outil d'aide à la décision permettant d'orienter rapidement l'analyse et de prioriser les actions, sans prétendre fournir une mesure précise du risque. Elle traduit ainsi une analyse complexe en une lecture claire, synthétique et exploitable de la posture de sécurité de l'organisation.

4.4.2 Structure de la représentation graphique

La représentation visuelle retenue repose sur la structure analytique définie à la section 4.2, soit le croisement des fonctions de sécurité et des familles de contrôles. Elle prend la forme d'une matrice composée de douze cellules, correspondant à l'ensemble des combinaisons possibles entre les quatre fonctions de sécurité, soit empêcher, détecter, retarder et répondre,

et les trois familles de contrôles, soit les contrôles technologiques, équipements et services, administratifs et procéduraux, ainsi que les contrôles humains.

À l'intérieur de chacune de ces cellules, les résultats agrégés ne sont pas présentés sous forme de valeurs numériques, mais au moyen d'une représentation graphique qualitative. Chaque cellule contient un diagramme circulaire en forme de beigne illustrant la distribution des niveaux d'implémentation des contrôles qui y sont associés. Cette distribution repose sur l'échelle définie à la section 4.3.3, allant de 0 à 3, à laquelle s'ajoute la possibilité d'exclure les contrôles jugés non applicables. Les segments du diagramme représentent la proportion relative des contrôles correspondant à chacun des niveaux d'implémentation.

Une codification par couleur est utilisée afin de faciliter la lecture : les contrôles pleinement implantés sont représentés en vert, ceux partiellement implantés en orange, ceux faiblement implantés en jaune, et les contrôles absents en rouge. Les contrôles identifiés comme non applicables ne sont pas pris en compte dans la représentation. Ce mode de représentation permet de conserver l'information relative à la distribution des niveaux d'implémentation sans la réduire à un indicateur unique, offrant ainsi une lecture plus nuancée de la posture de sécurité.

Enfin, la structure matricielle permet de situer ces résultats dans leur contexte fonctionnel et organisationnel, en reliant chaque distribution à une fonction de sécurité précise et à une famille de contrôles donnée. L'ensemble constitue une représentation cohérente de la posture de sécurité, permettant d'observer simultanément la répartition des contrôles et leur niveau d'implantation à travers les différentes dimensions du modèle.

4.4.3 Interprétation stratégique des résultats

L'interprétation de la représentation graphique ne vise pas à mesurer la performance de l'organisation en termes absolus, mais à apprécier la cohérence globale de la posture de sécurité à travers les différentes fonctions et familles de contrôles. L'objectif principal est d'obtenir, en

un coup d'œil, une compréhension synthétique de la manière dont les contrôles de sécurité sont répartis et implantés, afin d'identifier les déséquilibres structurels susceptibles d'affaiblir la capacité de l'organisation à faire face aux événements indésirables.

La lecture de la matrice doit d'abord s'effectuer à un niveau global, en observant la distribution des couleurs à travers l'ensemble des cellules. Une répartition relativement homogène des niveaux d'implémentation, même si elle se situe à un niveau intermédiaire, traduit généralement une posture de sécurité cohérente. À l'inverse, une alternance marquée entre des cellules fortement implantées et d'autres présentant des lacunes importantes met en évidence un déséquilibre structurel. Dans cette perspective, une matrice composée majoritairement de niveaux intermédiaires peut être jugée plus robuste qu'une matrice combinant des zones très fortes et des zones complètement déficientes, puisque la cohérence des mesures contribue directement à l'efficacité globale du dispositif de sécurité.

L'analyse doit également porter sur les écarts entre les fonctions de sécurité. Une concentration des contrôles dans les fonctions empêcher et détecter, sans capacité équivalente à retarder ou à répondre, constitue une faiblesse importante, puisqu'elle limite la capacité de l'organisation à réagir efficacement à un incident. De la même manière, un déséquilibre entre les familles de contrôles, par exemple une dépendance excessive aux solutions technologiques au détriment des mesures administratives ou humaines, peut compromettre la robustesse du dispositif, en créant des vulnérabilités liées à l'absence d'encadrement ou de comportements adaptés.

Dans ce contexte, l'acceptation d'un certain niveau de risque peut se traduire par une présence accrue de niveaux d'implémentation plus faibles, mais cette situation doit demeurer cohérente à l'échelle de l'ensemble de la matrice. Une dégradation uniforme est généralement moins problématique qu'une concentration de faiblesses dans une dimension particulière, qui constitue alors un point de rupture potentiel dans la posture de sécurité.

Lorsque des déséquilibres sont observés, la représentation globale permet d'orienter l'analyse vers des niveaux de détail plus fins. Il devient alors possible d'examiner la posture par domaine

de la sécurité, notamment la sécurité physique, la cybersécurité ou le filtrage de sécurité des personnes, afin d'identifier plus précisément l'origine des écarts. Si nécessaire, l'analyse peut être poursuivie à un niveau encore plus granulaire en s'intéressant aux résultats associés à des événements indésirables spécifiques, conformément à la logique de déclinaison présentée précédemment.

Ainsi, la représentation graphique ne constitue pas un outil de validation définitive de l'efficacité des mesures de sécurité, mais un instrument d'aide à la décision permettant de mettre en évidence, rapidement et de manière structurée, les forces, les faiblesses et les incohérences du dispositif en place. Elle fournit une base objective pour orienter les priorités d'amélioration, en privilégiant une approche axée sur la cohérence globale plutôt que sur l'accumulation de contrôles isolés.

CHAPITRE 5

VALIDATION EMPIRIQUE ET VALIDATION DES RÉSULTATS

Le présent chapitre vise à présenter les différentes démarches de validation réalisées dans le cadre de cette recherche ainsi qu'à analyser les principaux résultats obtenus. L'objectif principal de ces validations était de déterminer si le cadre d'analyse proposé permettait réellement :

- d'obtenir une représentation cohérente de la posture globale de sécurité;
- d'identifier certains déséquilibres entre les fonctions et axes de sécurité;
- de faciliter la compréhension des enjeux de sécurité;
- et de soutenir la prise de décision dans différents contextes organisationnels.

Afin de valider l'outil développé, plusieurs approches complémentaires ont été utilisées. Une première validation a été réalisée dans un environnement corporatif complexe auprès de l'entreprise Bombardier afin d'évaluer la pertinence du modèle dans une grande organisation disposant déjà de structures de sécurité matures. Une seconde expérimentation terrain a ensuite été effectuée auprès d'une PME québécoise afin d'évaluer l'applicabilité de l'outil dans un contexte organisationnel possédant des ressources plus limitées et une réalité opérationnelle différente. Finalement, un sondage de validation a été réalisé auprès de professionnels de différents domaines de la sécurité afin de recueillir leur perception concernant l'utilité, le caractère novateur et la pertinence de l'approche proposée.

Les différentes validations réalisées ont également permis d'identifier plusieurs constats méthodologiques importants concernant :

- la structuration des contrôles;
- les limites des référentiels existants;
- les difficultés associées à la catégorisation des contrôles;
- l'objectivité des mécanismes de cotation;

- ainsi que les enjeux liés à l'utilisabilité de l'outil dans différents contextes organisationnels.

Ce chapitre présente donc successivement :

- la validation de l'outil dans un environnement corporatif complexe;
- la validation dans un environnement PME;
- ainsi que l'analyse des résultats du sondage de validation réalisé auprès de professionnels de la sécurité.

5.1 Validation de l'outil dans un environnement corporatif complexe

L'outil développé dans le cadre du présent mémoire a été testé dans deux sites d'importance appartenant à l'entreprise Bombardier, en collaboration avec le directeur de la sécurité de l'organisation, M. Carol Gagnon. M. Gagnon œuvre chez Bombardier depuis 2007 et possède une expérience significative dans la gestion de la sécurité au sein d'environnements corporatifs complexes.

L'objectif de cette démarche n'était pas d'effectuer une évaluation exhaustive des dispositifs de sécurité de Bombardier, ni de porter un jugement sur les mesures en place, mais plutôt de valider la pertinence et l'utilité de l'outil développé dans un contexte réel. De plus, pour des raisons évidentes de sécurité et de protection de l'information, les détails précis des analyses réalisées, les caractéristiques des sites évalués ainsi que certains résultats spécifiques ne seront pas présentés dans ce mémoire, afin d'éviter de compromettre la sécurité des personnes, des infrastructures ou de l'information.

L'analyse réalisée consistait à valider la présence et le niveau d'implémentation de différents contrôles de sécurité, lesquels étaient catégorisés selon les fonctions de sécurité ainsi que selon les familles de contrôles. Les contrôles évalués couvraient également les trois domaines intégrés au modèle développé, soit le filtrage de sécurité des personnes, la sécurité physique et la cybersécurité.

Même si l'outil développé visait principalement des organisations de plus petite taille, notamment des PME ne disposant pas nécessairement d'équipes spécialisées en sécurité, l'utilisation de celui-ci dans un environnement corporatif mature représentait une occasion intéressante de confronter le modèle à une réalité organisationnelle plus complexe. Le regard d'un dirigeant expérimenté comme M. Gagnon permettait également d'obtenir une rétroaction stratégique sur la pertinence de l'approche proposée.

À la suite de l'analyse, M. Gagnon a notamment souligné le caractère novateur de l'intégration, au sein d'une même analyse, de la sécurité physique, de la cybersécurité et du filtrage de sécurité, alors que ces domaines sont habituellement traités séparément dans les organisations. Il a également mentionné que la catégorisation des contrôles selon les fonctions de sécurité et les familles de contrôles permettait d'obtenir une vision globale et cohérente de la posture de sécurité. Selon lui, la représentation visuelle proposée facilite l'identification rapide des forces, des faiblesses et des déséquilibres présents dans le dispositif de sécurité. Finalement, il a indiqué considérer cette approche comme un complément potentiellement intéressant aux méthodes déjà utilisées au sein de Bombardier.

Les observations réalisées dans le cadre de cette démarche ont également permis de confirmer plusieurs constats présentés précédemment dans la revue de littérature ainsi que dans le cadre théorique du mémoire. Lors de la préparation de la liste de contrôles utilisée dans l'outil, il a notamment été constaté que plusieurs contrôles fréquemment retrouvés dans la littérature ou dans les référentiels existants étaient difficiles à catégoriser clairement selon les fonctions de sécurité et les familles de contrôles proposées dans le présent mémoire. Cette situation tend également à confirmer l'hypothèse selon laquelle plusieurs listes de contrôles utilisées dans les référentiels et démarches de conformité reposent principalement sur une logique documentaire ou normative, sans nécessairement structurer les contrôles selon une perspective opérationnelle cohérente inspirée d'une logique de type adversary sequence diagram (ASD), où chaque contrôle contribue à une séquence globale de protection.

Dans ce contexte, plusieurs contrôles ont dû être adaptés, précisés ou créés afin de permettre leur intégration dans la structure analytique proposée. Cette situation a été particulièrement observée dans les fonctions détecter, retarder et répondre, ainsi que dans les familles administratives et procédurales et humaines. Ce constat rejoint directement les observations présentées précédemment concernant le déséquilibre fréquent entre les investissements technologiques et les autres dimensions de la sécurité.

À titre d'exemple, plusieurs organisations de normalisation et de conformité imposent l'utilisation de mots de passe longs et complexes afin de limiter les accès non autorisés. Toutefois, même si cette mesure contribue à la fonction empêcher dans la famille technologique, la capacité réelle de détecter une attaque demeure souvent limitée, particulièrement dans les PME. Bien que certaines grandes organisations disposent de centres d'opérations de sécurité (SOC) ou de mécanismes avancés de surveillance, ces approches sont difficilement transposables dans des environnements de plus petite taille. Cette situation met également en évidence une limite importante de plusieurs cadres normatifs et démarches de conformité, dont les contrôles sont souvent élaborés pour des structures organisationnelles importantes disposant de ressources spécialisées. Dans ce contexte, les contrôles de base proposés sont fréquemment présentés de manière isolée, sans nécessairement être structurés selon une logique stratégique globale permettant d'assurer une cohérence entre les fonctions empêcher, détecter, retarder et répondre. Cette réalité renforce l'importance d'adapter les contrôles de sécurité au contexte opérationnel réel des organisations plutôt que de reproduire des modèles difficilement applicables ou incomplets sur le plan fonctionnel.

Les visites ont également permis d'identifier certains enjeux liés à l'utilisation pratique de l'outil. En l'absence de questionnaire préparatoire ou de mécanisme préalable de collecte d'information, les gestionnaires rencontrés ne disposaient pas toujours des informations nécessaires pour confirmer si certains contrôles étaient effectivement implantés ou non. De plus, la demande visant à attribuer directement une cote numérique de 0 à 3 au niveau d'implantation des contrôles s'est révélée particulièrement subjective. Cette observation suggère qu'une évolution future de l'outil devrait privilégier des questions formulées dans un

langage simple et accessible pour les répondants, tout en générant automatiquement la valeur numérique associée en arrière-plan.

Il a également été observé que plusieurs contrôles relèvent de responsabilités réparties entre différents secteurs organisationnels, notamment la sécurité physique, la cybersécurité ou le filtrage de sécurité des personnes. Dans plusieurs cas, le gestionnaire responsable du site ne possédait pas l'ensemble des réponses nécessaires à l'évaluation complète des contrôles. Cette situation laisse entrevoir la pertinence d'un mécanisme permettant de rediriger automatiquement certaines questions vers les responsables concernés selon le domaine de sécurité visé.

Finalement, la démarche d'évaluation ainsi que la représentation graphique produite ont démontré une valeur pédagogique importante auprès des gestionnaires rencontrés. La catégorisation des contrôles selon les fonctions de sécurité et les familles de contrôles a notamment permis une meilleure compréhension du rôle réel des mesures de sécurité et de leur interdépendance. Il est apparu clairement que la présence de contrôles de détection, sans mécanismes de retardement ou de réponse adéquats, limite fortement l'efficacité globale du dispositif de sécurité.

L'exemple des défibrillateurs externes automatisés (DEA) illustre particulièrement bien cette logique. La simple présence d'un DEA dans un environnement ne garantit pas une capacité d'intervention efficace. Encore faut-il qu'un événement nécessitant son utilisation puisse être détecté rapidement, que des mécanismes permettent d'alerter les services d'urgence, que des procédures claires encadrent son utilisation et que des personnes présentes dans l'environnement aient reçu une formation adéquate. Cet exemple démontre concrètement l'importance d'une approche intégrée où les fonctions de sécurité et les différentes familles de contrôles doivent être considérées de manière complémentaire et cohérente.

5.2 Validation de l'outil dans un environnement PME

Afin de valider l'applicabilité du cadre d'analyse proposé dans un contexte réel, une expérimentation terrain a été réalisée auprès de SportVac, une PME québécoise spécialisée dans les voyages sportifs haut de gamme et les expériences VIP.

La démarche de validation s'est déroulée en plusieurs étapes. Une première rencontre a d'abord été réalisée avec les deux propriétaires de l'entreprise afin de présenter les objectifs du projet de recherche ainsi que le fonctionnement général de la matrice d'analyse. Par la suite, une seconde rencontre à distance a permis d'identifier les principaux événements indésirables préoccupant les dirigeants de l'entreprise. À partir de ces événements, une liste de contrôles de sécurité a ensuite été élaborée et répartie selon les 12 segments de la matrice.

Une rencontre subséquente a ensuite été réalisée directement dans les installations de l'entreprise afin de procéder à l'analyse détaillée des contrôles. Au total, près de 200 contrôles ont été évalués avec les deux propriétaires de l'entreprise. Finalement, les résultats obtenus ont été compilés dans la matrice graphique puis présentés aux dirigeants afin d'obtenir leur rétroaction concernant la compréhension des résultats, la pertinence de l'outil ainsi que son applicabilité dans un contexte réel de PME.

5.2.1 Constats méthodologiques issus de l'expérimentation

Cette expérimentation a rapidement permis de constater une difficulté méthodologique importante : il n'existe actuellement que très peu de référentiels permettant d'associer directement des contrôles de sécurité à des événements indésirables précis dans une logique globale et multidisciplinaire.

Bien qu'un grand nombre de normes, cadres méthodologiques, guides de bonnes pratiques et référentiels existent dans différents domaines de la sécurité, ceux-ci demeurent généralement spécialisés, fragmentés et fortement orientés vers certains secteurs particuliers comme la cybersécurité ou la sécurité physique. De plus, la qualité, la profondeur et la crédibilité de

plusieurs référentiels disponibles varient considérablement, particulièrement dans certains domaines moins structurés.

Cette réalité a rendu particulièrement complexe le travail d'identification et de sélection des contrôles applicables aux différents événements indésirables retenus dans le cadre de l'expérimentation. Ce constat vient d'ailleurs renforcer l'une des orientations principales de cette recherche, soit la pertinence de développer des référentiels structurés permettant d'associer plus uniformément les contrôles de sécurité aux différents types d'événements indésirables.

Une seconde difficulté méthodologique importante concernait la classification des contrôles dans les 12 segments de la matrice. Même lorsqu'un contrôle était identifié, il demeurait souvent difficile de déterminer précisément :

- sa fonction principale;
- son axe d'intervention;
- ainsi que son impact réel sur la posture globale de sécurité.

Les contrôles associés aux fonctions empêcher et détecter étaient généralement relativement faciles à identifier, particulièrement en cybersécurité et en sécurité physique. À l'inverse, les contrôles liés aux fonctions retarder et répondre étaient beaucoup plus difficiles à trouver dans les référentiels existants et devaient fréquemment être développés, adaptés ou interprétés spécifiquement pour les besoins de la matrice.

Le constat était encore plus marqué concernant le filtrage de sécurité. Très peu de référentiels opérationnels, de cadres méthodologiques ou de listes de contrôles standardisés ont pu être identifiés dans ce domaine. Dans plusieurs cas, les contrôles associés au filtrage de sécurité ont donc dû être créés entièrement à partir de zéro afin de permettre leur intégration dans la matrice d'analyse.

Finalement, l'expérimentation a également démontré les limites importantes associées à l'utilisation d'une cotation subjective sur une échelle de 0 à 3 afin de valider les contrôles. Cette approche s'est révélée difficile à interpréter pour les répondants et introduisait un niveau important de subjectivité dans les réponses. Deux personnes différentes pouvaient ainsi attribuer des résultats différents à une même situation selon leur propre perception du niveau de maturité du contrôle évalué.

Ces constats ont permis d'identifier la nécessité d'utiliser des réponses beaucoup plus objectives, contextualisées et standardisées afin d'améliorer la cohérence, la reproductibilité et la rigueur méthodologique de l'outil proposé.

L'expérimentation a également démontré qu'un même contrôle pouvait avoir un impact sur plusieurs événements indésirables simultanément. Certains contrôles fondamentaux contribuaient simultanément à réduire plusieurs risques différents et devaient donc être comptabilisés plusieurs fois dans l'outil afin de mieux représenter leur importance réelle dans la posture globale de sécurité. Ce constat fut particulièrement important dans le développement de la pondération des contrôles.

L'analyse réalisée auprès de SportVac a également permis de confirmer l'une des hypothèses centrales de cette recherche, soit l'existence d'un déséquilibre fréquent entre les différents axes de sécurité. L'organisation possédait plusieurs contrôles technologiques jugés intéressants, mais les procédures documentées apparaissaient beaucoup moins développées. Cette observation rejoint directement l'hypothèse selon laquelle les organisations tendent à investir davantage dans les équipements, technologies et services que dans les procédures ou le facteur humain.

L'expérimentation terrain a également permis d'identifier plusieurs enjeux liés à l'utilisabilité de l'outil dans un contexte PME. L'un des constats les plus importants concerne le niveau de langage utilisé dans les questions et les contrôles. Il est rapidement apparu que plusieurs concepts de sécurité demeuraient trop techniques pour des propriétaires ou gestionnaires ne

possédant pas une expertise spécialisée en sécurité. Cette réalité suggère qu'une éventuelle plateforme d'auto-évaluation devrait utiliser un vocabulaire beaucoup plus accessible et simplifié.

Un autre constat important concerne l'effet intimidant que peut produire une liste complète de contrôles avancés auprès des PME. Le fait de présenter simultanément des contrôles de base ainsi que des mécanismes techniques avancés peut rapidement donner l'impression aux gestionnaires que leur posture de sécurité est catastrophique, même lorsqu'elle demeure supérieure à celle de plusieurs autres PME comparables.

L'expérimentation a donc permis d'identifier la pertinence potentielle d'un modèle de progression par niveaux de maturité, par exemple :

- Niveau 1 : PME sensibilisée;
- Niveau 2 : PME sécurisée;
- Niveau 3 : PME renforcée.

Cette approche permettrait aux organisations de progresser graduellement sans être découragées dès les premières étapes de l'analyse.

L'expérimentation a également démontré l'importance de permettre le routage de certaines questions vers des experts externes. Dans le cas de SportVac, plusieurs composantes liées à la cybersécurité étaient gérées par des fournisseurs spécialisés externes. Les dirigeants de l'entreprise ne détenaient donc pas toujours l'information technique nécessaire pour répondre précisément à certaines questions. Une future plateforme pourrait donc permettre de transmettre automatiquement certaines sections à des fournisseurs externes responsables de domaines particuliers.

5.2.2 Perception et rétroaction des dirigeants de la PME

À la suite de l'expérimentation, les dirigeants de SportVac ont été invités à fournir une rétroaction qualitative concernant leur expérience globale ainsi que leur perception de l'outil proposé. Les commentaires obtenus furent particulièrement positifs et viennent soutenir plusieurs hypothèses de cette recherche.

Les dirigeants ont notamment indiqué que :

- l'expérience globale avait été appréciée;
- la représentation graphique permettait de visualiser rapidement les points faibles;
- l'approche globale était pertinente et facile à comprendre;
- les besoins en procédures, formations et accompagnement demeuraient importants;
- et qu'une plateforme d'auto-évaluation simplifiée pourrait réellement contribuer à améliorer la posture de sécurité des PME québécoises.

Les commentaires recueillis démontrent également que les dirigeants percevaient actuellement un manque important d'accompagnement en matière de sécurité pour les PME québécoises. Ceux-ci ont notamment indiqué que les ressources disponibles leur semblaient floues, peu accessibles et insuffisamment adaptées à leur réalité opérationnelle.

Les dirigeants ont également démontré un fort intérêt envers :

- des recommandations automatisées;
- des modèles de procédures;
- des formations modulaires;
- ainsi qu'un modèle de progression adapté aux PME.

La représentation graphique remise à l'entreprise semble également avoir constitué l'un des éléments les plus appréciés de l'expérimentation. Les dirigeants ont mentionné que celle-ci permettait d'identifier rapidement les forces et faiblesses de leur posture de sécurité globale,

facilitant ainsi la compréhension des déséquilibres existants entre les différents axes de sécurité.

Les commentaires obtenus suggèrent également qu'un éventuel développement de la plateforme pourrait dépasser le simple cadre d'analyse pour devenir également un outil :

- d'accompagnement;
- de sensibilisation;
- de formation;
- et de maturation progressive de la posture de sécurité organisationnelle des PME.

Finalement, cette expérimentation a permis de valider non seulement la faisabilité générale du modèle proposé, mais également sa pertinence dans un contexte réel de PME. Les différents constats méthodologiques observés durant l'expérimentation ont permis d'identifier plusieurs pistes d'amélioration importantes concernant la structuration des référentiels, la classification des contrôles, l'objectivité des réponses ainsi que l'adaptation de l'outil aux réalités opérationnelles des PME québécoises.

L'expérimentation a également démontré que la représentation graphique proposée facilite la compréhension globale de la posture de sécurité et permet d'identifier rapidement certains déséquilibres entre les différents axes (familles) et fonctions de sécurité. Les réactions obtenues auprès des dirigeants de l'entreprise suggèrent finalement qu'une approche simplifiée, progressive et multidisciplinaire pourrait contribuer à rendre la sécurité globale plus accessible aux PME tout en favorisant une meilleure compréhension des interactions entre les différents domaines de sécurité.

5.3 Présentation et analyse des résultats du sondage de validation

Cette section présente les résultats du sondage réalisé lors de l'événement du 12 mai 2026 organisé à l'École de technologie supérieure (ÉTS). Ce sondage visait à recueillir l'opinion de professionnels de la sécurité concernant la pertinence, l'utilité et le caractère novateur du cadre

d'analyse de la posture de sécurité globale développé dans le cadre de cette recherche. Le questionnaire visait également à documenter la perception des experts quant aux déséquilibres existants dans les organisations en matière de sécurité, notamment entre les différentes fonctions de sécurité ainsi qu'entre les différents domaines d'expertise.

L'événement prenait la forme d'un cocktail dînatoire accompagné d'activités de réseautage multidisciplinaires, suivi d'une conférence présentant les travaux de recherche ainsi que le cadre d'analyse développé dans le cadre de cette maîtrise. L'objectif principal de l'événement était de favoriser les échanges entre les différents domaines de la sécurité et de présenter une approche visant à réduire le travail en silo traditionnellement observé entre la cybersécurité, la sécurité physique, la sécurité de l'information et le filtrage de sécurité.

L'événement était organisé en collaboration avec plusieurs organismes reconnus du domaine de la sécurité au Québec, notamment :

- Cybereco
- ASIS International - Chapitre de la province de Québec
- CANASA
- ISC2 Montréal Chapter
- ASIMM

La participation de ces organisations contribuait à renforcer la crédibilité de l'événement ainsi que la diversité des expertises représentées parmi les participants.

Par ailleurs, la directrice de la sécurité de l'information du ministère de la Cybersécurité et du Numérique, Mme Bianca Lavoie, était présente lors de l'événement. Une vidéo personnalisée du vice-premier ministre et ministre de la Sécurité publique du Québec, M. Ian Lafrenière, a également été diffusée puisqu'il ne pouvait être présent sur place.

Les interventions de ces représentants gouvernementaux mettaient notamment l'accent sur l'importance de réduire le travail en silo entre les différents domaines de la sécurité et

d'augmenter la collaboration interdisciplinaire afin d'améliorer la posture globale de sécurité des organisations québécoises. Cette orientation rejoint directement les fondements conceptuels du cadre d'analyse proposé dans cette recherche.

5.3.1 Méthodologie du sondage

Afin de recueillir l'opinion de professionnels de la sécurité concernant le cadre d'analyse proposé dans cette recherche, un sondage de validation a été réalisé lors de l'événement du 12 mai 2026 organisé à l'École de technologie supérieure (ÉTS). Le questionnaire a été conçu à l'aide de la plateforme Microsoft Forms et diffusé directement aux participants durant l'événement à l'aide d'un lien Web et d'un code QR affichés pendant la présentation. Les participants pouvaient répondre au questionnaire à partir de leur téléphone mobile ou de leur ordinateur personnel. Le questionnaire utilisé dans le cadre du sondage ainsi qu'un résumé visuel des résultats générés à partir de Microsoft Forms sont présentés à l'ANNEXE II.

Le sondage était entièrement anonyme et aucune information nominative permettant d'identifier les participants n'a été recueillie. Le questionnaire est demeuré accessible pendant une période approximative de 30 minutes suivant la présentation du cadre d'analyse afin de permettre aux participants de répondre alors que les concepts présentés étaient encore récents dans leur mémoire.

Le questionnaire comportait 25 questions réparties en plusieurs sections portant notamment sur :

- le profil professionnel des répondants;
- leur niveau d'expérience;
- leur perception des déséquilibres organisationnels en sécurité;
- leur perception des domaines de sécurité négligés;
- la compréhension des interactions entre les domaines de sécurité;
- l'utilité opérationnelle du cadre proposé;
- le caractère novateur de la représentation visuelle;

- ainsi que la pertinence générale de l'approche holistique proposée.

Le questionnaire comprenait principalement des questions utilisant une échelle de Likert à quatre niveaux :

- pas du tout d'accord;
- plutôt en désaccord;
- plutôt d'accord;
- tout à fait d'accord.

Le choix d'une échelle à quatre niveaux visait à limiter les réponses neutres et à encourager un positionnement plus clair des participants concernant les différents énoncés proposés. Certaines questions ouvertes et conditionnelles permettaient également aux participants de préciser certaines réponses ou d'ajouter des commentaires qualitatifs sur le cadre d'analyse présenté. Au total, 45 répondants ont complété le questionnaire et les données recueillies ont ensuite été compilées et analysées afin d'identifier les principales tendances observées ainsi que les éléments soutenants ou infirmant les hypothèses de cette recherche.

5.3.2 Profil des répondants

Le sondage a été complété par 45 répondants provenant de plusieurs domaines de la sécurité. Les domaines d'expertise principaux identifiés par les participants étaient :

- Sécurité physique : 27 répondants (60,0 %)
- Cybersécurité : 13 répondants (28,9 %)
- Gestion ou direction : 11 répondants (24,4 %)
- Enquête : 9 répondants (20,0 %)
- Sécurité de l'information : 8 répondants (17,8 %)
- Filtrage de sécurité : 6 répondants (13,3 %)

Puisque certaines personnes possédaient plusieurs expertises, un même répondant pouvait sélectionner plus d'un domaine. La forte représentation de professionnels issus de la sécurité

physique est cohérente avec le contexte de l'événement ainsi qu'avec les organisations partenaires impliquées dans celui-ci. Toutefois, la présence simultanée de spécialistes provenant de plusieurs secteurs renforce la pertinence des observations recueillies dans le cadre d'une approche holistique de la sécurité.

Le niveau d'expérience des répondants était également élevé :

- 0 à 5 ans d'expérience : 10 répondants (22,2 %)
- 5 à 10 ans : 6 répondants (13,3 %)
- 10 à 20 ans : 13 répondants (28,9 %)
- Plus de 20 ans : 16 répondants (35,6 %)

Ainsi, 29 répondants sur 45 (64,5 %) possédaient plus de 10 années d'expérience dans leur domaine respectif. Ce résultat contribue à renforcer la crédibilité des observations recueillies, puisque les répondants provenaient majoritairement du terrain et possédaient une expérience significative en gestion ou en opération de sécurité.

5.3.3 Perception de l'état actuel de la sécurité organisationnelle

Les résultats démontrent une perception largement partagée selon laquelle les organisations présentent actuellement des déséquilibres importants dans leur approche de la sécurité. À l'affirmation selon laquelle « les organisations sont suffisamment préparées à détecter et intervenir avant compromission », la moyenne obtenue fut de 2,13 sur 4. Les réponses se répartissaient comme suit :

- Pas du tout d'accord : 13 répondants (28,9 %)
- Plutôt en désaccord : 23 répondants (51,1 %)
- Plutôt d'accord : 9 répondants (20,0 %)
- Tout à fait d'accord : 0 répondant (0 %)

Ainsi, 36 répondants sur 45 (80,0 %) considéraient que les organisations ne sont pas suffisamment préparées à détecter et intervenir avant la compromission des actifs. Ce résultat

constitue l'un des constats les plus importants du sondage puisqu'il soutient directement l'hypothèse centrale de cette recherche voulant que plusieurs organisations concentrent principalement leurs efforts sur des mesures préventives, au détriment des fonctions détecter, retarder et répondre.

5.3.4 Déséquilibre entre les axes organisationnels

À l'affirmation selon laquelle « les ressources sont réparties de manière équilibrée entre technologie, processus et facteur humain », la moyenne obtenue fut de 2,24 sur 4. Les réponses obtenues étaient :

- Pas du tout d'accord : 9 répondants (20,0 %)
- Plutôt en désaccord : 20 répondants (44,4 %)
- Plutôt d'accord : 15 répondants (33,3 %)
- Tout à fait d'accord : 1 répondant (2,2 %)

Ainsi, 29 répondants sur 45 (64,4 %) percevaient un déséquilibre dans la répartition des ressources de sécurité. Ce résultat appuie directement la logique de la matrice proposée dans cette recherche, basée sur trois axes complémentaires :

- les technologies et équipements;
- les procédures;
- le facteur humain.

Les résultats semblent démontrer que les organisations ont tendance à concentrer leurs investissements dans certains axes, particulièrement les technologies, au détriment des dimensions procédurales et humaines.

5.3.5 Compréhension limitée des interactions entre les domaines

À l'affirmation selon laquelle « la direction comprend bien les interactions entre les différentes composantes de sécurité », la moyenne obtenue fut de 2,22 sur 4. Les réponses étaient :

- Pas du tout d'accord : 10 répondants (22,2 %)
- Plutôt en désaccord : 19 répondants (42,2 %)
- Plutôt d'accord : 14 répondants (31,1 %)
- Tout à fait d'accord : 2 répondants (4,4 %)

Ainsi, 29 répondants sur 45 (64,4 %) considéraient que les dirigeants comprennent mal les interactions entre les différents domaines de sécurité. Ce constat soutient directement l'idée selon laquelle les organisations fonctionnent encore largement en silo.

5.3.6 Domaine perçu comme le plus négligé

Les répondants devaient identifier le domaine qu'ils considéraient comme étant le plus négligé dans les organisations. Les résultats obtenus furent :

- Filtrage de sécurité : 21 réponses (46,7 %)
- Sécurité physique : 13 réponses (28,9 %)
- Cybersécurité : 8 réponses (17,8 %)
- Aucun : 3 réponses (6,7 %)

Le filtrage de sécurité apparaît donc comme le domaine le plus fréquemment perçu comme étant négligé. Cependant, une observation particulièrement intéressante ressort de l'analyse croisée des réponses : plusieurs répondants avaient tendance à considérer leur propre domaine d'expertise comme étant le domaine le plus négligé.

Par exemple :

- plusieurs experts en sécurité physique identifiaient la sécurité physique comme sous-estimée;
- les spécialistes du filtrage de sécurité identifiaient majoritairement le filtrage comme étant négligé;
- certains experts en cybersécurité considéraient également leur domaine comme insuffisamment pris en compte.

Cette tendance suggère l'existence de biais disciplinaires dans l'évaluation de la sécurité organisationnelle. Chaque domaine tend naturellement à percevoir ses propres enjeux comme étant les plus critiques ou les plus sous-estimés. Cette dynamique peut contribuer à maintenir des approches fragmentées et à favoriser des investissements concentrés dans certains silos plutôt qu'une approche équilibrée de la sécurité.

5.3.7 Contribution de la matrice à la réduction des biais disciplinaires

Les résultats du sondage suggèrent que la matrice proposée pourrait contribuer à réduire ce type de biais. Contrairement aux approches traditionnelles centrées sur des domaines spécifiques tels que la cybersécurité, la sécurité physique ou le filtrage de sécurité, la matrice développée dans cette recherche repose sur quatre fonctions universelles de sécurité ainsi que sur trois axes organisationnels applicables à l'ensemble des domaines.

L'analyse ne repose donc pas directement sur des silos disciplinaires, mais plutôt sur une logique fonctionnelle uniforme. Cette approche semble permettre :

- une analyse plus neutre;
- une meilleure visualisation des déséquilibres;
- une réduction de l'influence des biais professionnels;
- une meilleure répartition des investissements en sécurité.

Ainsi, plutôt que de demander si une organisation investit suffisamment dans un domaine précis, la matrice permet d'évaluer si l'organisation dispose de contrôles équilibrés permettant :

- d'empêcher;
- de détecter;
- de retarder;
- de répondre;

et ce, à travers :

- les technologies;
- les procédures;
- le facteur humain.

5.3.8 Validation de l'utilité du modèle

Les résultats obtenus concernant l'utilité du modèle furent particulièrement élevés.

À l'affirmation selon laquelle le modèle « facilite la compréhension globale de la posture de sécurité », la moyenne obtenue fut de 3,73 sur 4 et 45 répondants sur 45 (100 %) se disaient en accord ou fortement en accord.

L'affirmation selon laquelle le modèle « permet d'identifier rapidement les forces » a obtenu une moyenne de 3,78 sur 4 avec 45 répondants sur 45 (100 %) en accord ou fortement en accord.

L'affirmation selon laquelle le modèle « permet d'identifier rapidement les faiblesses » a également obtenu une moyenne de 3,78 sur 4 avec 44 répondants sur 45 (97,8 %) en accord ou fortement en accord.

L'énoncé selon lequel le modèle « permet de visualiser les déséquilibres » a obtenu la moyenne la plus élevée avec 3,82 sur 4 et 45 répondants sur 45 (100 %) en accord ou fortement en accord.

L'affirmation selon laquelle le modèle « facilite la communication auprès des décideurs » a obtenu une moyenne de 3,69 sur 4 avec 45 répondants sur 45 (100 %) en accord ou fortement en accord.

Finalement, l'affirmation selon laquelle le modèle « peut soutenir la prise de décision » a obtenu une moyenne de 3,71 sur 4 avec 44 répondants sur 45 (97,8 %) en accord ou fortement en accord.

Ces résultats démontrent un niveau d'adhésion très élevé envers le cadre d'analyse proposé. Les répondants semblent percevoir une forte valeur opérationnelle, pédagogique et décisionnelle dans la représentation visuelle proposée par la matrice.

5.3.9 Originalité perçue du modèle

À la question portant sur l'existence d'un outil similaire intégrant simultanément la cybersécurité, la sécurité physique et le filtrage de sécurité dans une même logique d'analyse, les résultats obtenus furent :

- Non : 43 répondants (95,6 %)
- Oui : 2 répondants (4,4 %)

La très grande majorité des participants affirmaient donc ne connaître aucun outil comparable. Ce résultat soutient directement le caractère novateur du modèle proposé dans cette recherche et semble confirmer l'existence d'un vide méthodologique dans les approches actuelles de gestion de la sécurité, particulièrement dans les PME.

Les deux répondants ayant affirmé connaître des approches comparables ont mentionné Circadian Risk ainsi que certaines normes ou cadres tels que les normes CMMC et le Programme de coordination de la cybersécurité canadienne (PCCC). Toutefois, ces réponses semblent davantage référer à des cadres spécialisés ou complémentaires qu'à un outil directement comparable au modèle proposé dans cette recherche.

Par exemple, Circadian Risk est principalement orienté vers l'analyse et la visualisation des risques liés à la sécurité physique et à la résilience organisationnelle. Bien que cette approche présente certaines similitudes au niveau de la représentation visuelle et de la centralisation de

l'information, elle ne semble pas reposer sur une logique uniforme intégrant simultanément les fonctions empêcher, détecter, retarder et répondre à travers les axes technologies, procédures et facteur humain.

De manière similaire, les normes CMMC ainsi que le PCCC canadien constituent principalement des cadres de conformité et de gouvernance orientés vers la cybersécurité et la protection des systèmes d'information. Bien qu'ils intègrent certaines dimensions humaines et procédurales, ces cadres demeurent principalement structurés autour des exigences de conformité et de maturité en cybersécurité plutôt qu'autour d'une analyse globale et équilibrée de la posture de sécurité organisationnelle.

Ces réponses semblent donc démontrer que les participants associent parfois des outils de gestion du risque, de conformité ou de gouvernance à des approches holistiques de sécurité, même lorsque ceux-ci demeurent spécialisés dans certains domaines particuliers. Ainsi, malgré certaines similitudes conceptuelles partielles, les résultats du sondage continuent de soutenir l'idée qu'il existe peu d'outils intégrant simultanément, la sécurité physique, la cybersécurité et le filtrage de sécurité dans une logique d'analyse fonctionnelle uniforme et visuellement intégrée telle que proposée dans cette recherche.

5.3.10 Limites méthodologiques du sondage

Certaines limites doivent néanmoins être considérées dans l'interprétation des résultats obtenus. L'échantillon demeure relativement limité avec 45 répondants et ne constitue pas un échantillon probabiliste représentatif de l'ensemble des professionnels de la sécurité. Les participants étaient également présents volontairement à un événement spécialisé portant précisément sur la sécurité globale, ce qui peut introduire certains biais favorables envers l'approche proposée.

De plus, plusieurs participants connaissaient déjà le chercheur avant l'événement, soit pour l'avoir rencontré lors d'événements professionnels antérieurs, dans un contexte

d’enseignement, de conférence ou de formation, soit par l’entremise des médias sociaux professionnels tels que LinkedIn ou encore par des interventions dans les médias traditionnels. Cette réalité peut avoir influencé certaines perceptions positives envers le modèle présenté.

Le questionnaire reposait également sur le principe de la bonne foi des répondants. Aucune validation indépendante n’a été réalisée concernant les années d’expérience déclarées, les certifications détenues ou les champs d’expertise sélectionnés par les participants. Les informations sociodémographiques et professionnelles utilisées dans l’analyse reposent donc exclusivement sur les déclarations des répondants.

Finalement, bien que le questionnaire ait été anonyme, le contexte même de la présentation pouvait également créer un biais de désirabilité sociale, certains participants pouvant être plus enclins à formuler des commentaires favorables dans un environnement professionnel public lié directement au sujet de recherche présenté.

Malgré ces limites, la cohérence des réponses obtenues ainsi que le niveau d’expérience déclaré par les répondants permettent néanmoins d’identifier plusieurs tendances fortes soutenant les hypothèses de cette recherche.

CHAPITRE 6

DISCUSSION ET ANALYSE

Le présent chapitre vise à interpréter les principaux résultats obtenus dans le cadre des différentes validations réalisées durant cette recherche. Contrairement au chapitre précédent, qui présentait principalement les résultats de manière descriptive, le présent chapitre propose une analyse transversale des constats recueillis afin d'identifier certaines tendances récurrentes, certains déséquilibres organisationnels ainsi que les principales contributions du cadre d'analyse proposé.

Les différentes validations réalisées, incluant les expérimentations terrain, le sondage auprès des professionnels de la sécurité ainsi qu'une analyse exploratoire des données recueillies, permettent de mettre en évidence plusieurs constats convergents concernant la gestion actuelle de la sécurité au sein des organisations. Les résultats obtenus suggèrent notamment l'existence de déséquilibres importants entre les différentes fonctions de sécurité, une forte dominance des approches technologiques, une difficulté persistante d'intégration entre les domaines de sécurité ainsi qu'un besoin accru d'outils facilitant la compréhension globale de la posture de sécurité organisationnelle.

6.1 Analyse exploratoire des perceptions des répondants

Afin d'approfondir l'interprétation des résultats obtenus lors du sondage présenté au chapitre précédent, une analyse exploratoire complémentaire des données recueillies a été réalisée. Cette démarche visait à identifier certaines structures de perception, certains regroupements de profils ainsi que certaines oppositions conceptuelles présentes parmi les répondants. Les analyses effectuées permettent notamment de mieux comprendre les perceptions liées à l'intégration des domaines de sécurité, à l'équilibre des mesures organisationnelles ainsi qu'à l'importance respective des différentes dimensions de la sécurité globale.

6.1.1 Présentation de l'ACM et de la CAH

Afin d'explorer les relations entre les différentes variables qualitatives du sondage, une analyse des correspondances multiples (ACM) ainsi qu'une classification ascendante hiérarchique (CAH) ont été réalisées. L'ACM constitue une méthode exploratoire permettant d'identifier certaines relations, oppositions et regroupements entre différentes modalités qualitatives au sein d'un jeu de données, alors que la CAH permet d'identifier des regroupements d'individus partageant des profils de réponses similaires. L'objectif de cette analyse n'était pas de produire une modélisation statistique généralisable à l'ensemble des organisations québécoises, mais plutôt d'explorer certaines structures de perception présentes chez les répondants et de vérifier si des tendances cohérentes avec les observations qualitatives réalisées dans le cadre de cette recherche pouvaient être observées.

L'analyse initiale a permis d'identifier la présence d'un individu atypique contribuant de manière disproportionnée à la construction du plan factoriel. Cet individu présentait des réponses systématiquement positives concernant l'intégration de la sécurité, l'équilibre des ressources ainsi que la maturité organisationnelle. Afin de limiter l'influence excessive de cette observation singulière sur l'interprétation globale des résultats, cette dernière a été retirée pour la suite de l'analyse exploratoire. L'analyse de l'inertie suggère également que les quatre premiers axes factoriels contiennent l'information la plus significative du jeu de données analysé. Les résultats obtenus demeurent toutefois de nature exploratoire et doivent être interprétés avec prudence en raison de la taille limitée de l'échantillon.

6.1.2 Principaux regroupements observés

L'ACM et la CAH ont permis d'identifier plusieurs regroupements distincts de répondants partageant certaines perceptions communes concernant l'état actuel de la sécurité organisationnelle. Un premier groupe associait fortement les organisations à des déséquilibres importants entre les différentes dimensions de la sécurité. Ce groupe était notamment caractérisé par une perception négative de l'intégration globale de la sécurité, de l'équilibre des ressources organisationnelles, de la compréhension des interactions entre les domaines de

sécurité ainsi que de la prise en compte du filtrage de sécurité. À l'opposé, un second groupe percevait les organisations comme étant davantage équilibrées et intégrées. Les répondants de ce groupe associaient notamment leurs réponses à une meilleure compréhension des interactions entre les domaines de sécurité, à un équilibre plus adéquat entre les fonctions de sécurité ainsi qu'à une meilleure intégration organisationnelle des différentes composantes de sécurité.

L'analyse met également en évidence certaines différences de perception selon les domaines d'expertise des répondants. Les profils provenant principalement de la sécurité physique et de la gestion organisationnelle associaient davantage la sécurité globale à l'importance du facteur humain, à la sécurité physique de l'information ainsi qu'à l'importance d'une approche multidisciplinaire intégrée. À l'inverse, certains profils provenant principalement de la cybersécurité identifiaient paradoxalement la cybersécurité elle-même comme étant un domaine encore insuffisamment pris en compte dans plusieurs organisations. Cette observation suggère que les perceptions des déséquilibres organisationnels peuvent varier selon les champs d'expertise des répondants ainsi que selon leur exposition opérationnelle aux différents types de menaces.

6.1.3 Oppositions conceptuelles observées

Les analyses réalisées mettent également en évidence certaines oppositions conceptuelles importantes entre différentes visions de la sécurité organisationnelle. D'une part, certains groupes de répondants associaient fortement la sécurité à une approche intégrée reposant sur l'équilibre entre les fonctions de sécurité, l'intégration des différents domaines ainsi qu'une meilleure prise en compte des dimensions humaines et organisationnelles. D'autre part, certains répondants percevaient encore la sécurité principalement sous un angle plus technologique ou spécialisé.

Ces oppositions observées dans les regroupements de perception viennent renforcer plusieurs constats déjà observés dans la littérature ainsi que dans les validations terrain réalisées dans le

cadre de cette recherche. Elles suggèrent également que les difficultés d'intégration entre les domaines de sécurité ne reposent pas uniquement sur des enjeux technologiques ou organisationnels, mais également sur des différences culturelles et conceptuelles entre les disciplines de sécurité elles-mêmes.

6.2 Analyse des principaux constats

Les différentes validations réalisées dans le cadre de cette recherche permettent de dégager plusieurs constats récurrents concernant la gestion contemporaine de la sécurité organisationnelle. Les résultats obtenus suggèrent notamment l'existence de déséquilibres importants entre les fonctions de sécurité, une forte dominance des approches technologiques ainsi qu'une difficulté persistante d'intégration entre les différents domaines de sécurité. Les sous-sections suivantes présentent une analyse détaillée des principaux constats observés.

6.2.1 Déséquilibre des mesures de sécurité

L'un des principaux constats issus des différentes validations réalisées concerne le déséquilibre fréquent des mesures de sécurité au sein des organisations. Les résultats du sondage ainsi que les validations terrain suggèrent que plusieurs organisations concentrent principalement leurs efforts sur certaines fonctions de sécurité, particulièrement les mesures préventives, au détriment des fonctions détecter, retarder et répondre. Cette tendance a également été observée dans les analyses exploratoires réalisées à partir des données du sondage, où certains regroupements de répondants associaient fortement les organisations à un manque d'équilibre entre les objectifs de sécurité ainsi qu'à une faible intégration des différentes dimensions de sécurité.

Ces constats apparaissent cohérents avec plusieurs observations effectuées durant les expérimentations terrain, où plusieurs contrôles étaient principalement orientés vers la prévention immédiate des incidents sans nécessairement offrir de mécanismes structurés de détection, de ralentissement ou d'intervention avant compromission. Cette situation semble également cohérente avec plusieurs cadres organisationnels actuels qui privilégient souvent

des approches centrées sur la conformité, les obligations réglementaires ou les exigences technologiques minimales, sans nécessairement assurer une couverture cohérente de l'ensemble des fonctions de sécurité. Les résultats obtenus dans le cadre de cette recherche suggèrent ainsi qu'une représentation structurée des mesures de sécurité selon les fonctions empêcher, détecter, retarder et répondre permet de mieux visualiser certains déséquilibres organisationnels souvent difficiles à identifier dans les approches traditionnelles de sécurité.

6.2.2 Dominance des technologies

Les résultats obtenus suggèrent également une forte dominance des approches technologiques dans la gestion contemporaine de la sécurité organisationnelle. Cette réalité apparaît autant dans la littérature que dans les validations terrain ainsi que dans les résultats du sondage. Plusieurs répondants associaient les organisations à une forte dépendance envers les solutions technologiques alors que les dimensions humaines, procédurales ou organisationnelles semblaient parfois moins structurées ou moins développées. Cette tendance semble particulièrement observable dans les PME, où les investissements en sécurité prennent fréquemment la forme d'acquisitions technologiques ponctuelles plutôt que d'une approche globale intégrant simultanément les processus organisationnels, la formation, la sensibilisation et la gouvernance de sécurité.

L'analyse exploratoire met également en évidence certaines différences importantes entre les groupes de répondants. Les profils issus de la sécurité physique et de la gestion organisationnelle associaient davantage la sécurité globale à l'importance du facteur humain et à la nécessité d'une approche multidisciplinaire intégrée. Ces résultats suggèrent que plusieurs déséquilibres organisationnels pourraient découler non seulement de contraintes budgétaires ou techniques, mais également de biais disciplinaires influençant la manière dont les risques sont perçus et priorisés à l'intérieur des organisations. Les validations réalisées dans le cadre de cette recherche tendent également à démontrer qu'une approche reposant uniquement sur les technologies demeure insuffisante pour assurer une protection cohérente

des organisations lorsque les procédures organisationnelles et les dimensions humaines ne sont pas intégrées de manière adéquate.

6.2.3 Difficulté d'intégration des domaines de sécurité

L'un des constats les plus importants de cette recherche concerne la difficulté persistante d'intégration entre les différents domaines de sécurité. Les validations réalisées suggèrent que la cybersécurité, la sécurité physique, la sécurité de l'information ainsi que le filtrage de sécurité demeurent encore fréquemment gérés de manière relativement indépendante à l'intérieur des organisations. Cette réalité favorise l'apparition de silos organisationnels limitant la circulation de l'information, la coordination des mesures de sécurité ainsi que la compréhension globale des risques.

Les résultats du sondage démontrent d'ailleurs qu'une proportion importante des répondants considérait que les organisations ne comprennent pas adéquatement les interactions existantes entre les différents domaines de sécurité. Les analyses exploratoires réalisées viennent également renforcer ce constat en mettant en évidence plusieurs regroupements de répondants présentant des perceptions très opposées concernant le niveau réel d'intégration organisationnelle. Ces résultats apparaissent cohérents avec plusieurs observations effectuées dans la littérature, où les cadres de cybersécurité, de sécurité physique et de sécurité de l'information sont souvent développés de manière relativement indépendante, avec des terminologies, des référentiels et des approches méthodologiques distinctes.

Les difficultés observées ne semblent donc pas uniquement technologiques. Elles apparaissent également liées à des différences culturelles, organisationnelles et conceptuelles entre les disciplines de sécurité elles-mêmes. Les résultats obtenus dans le cadre de cette recherche suggèrent ainsi qu'un cadre d'analyse commun permettant de visualiser simultanément plusieurs dimensions de la sécurité peut contribuer à faciliter les discussions interdisciplinaires et à améliorer la compréhension globale de la posture de sécurité organisationnelle.

6.2.4 Importance du facteur humain

Les résultats obtenus suggèrent également que le facteur humain occupe une place centrale dans la sécurité organisationnelle globale. Plusieurs regroupements observés dans l'ACM associaient fortement les perceptions positives d'une approche globale à l'importance du facteur humain, à la sensibilisation ainsi qu'à la compréhension organisationnelle des enjeux de sécurité. Cette observation rejoint plusieurs travaux de recherche démontrant que plusieurs incidents de sécurité impliquent directement ou indirectement des dimensions humaines telles que la négligence, les erreurs opérationnelles, l'ingénierie sociale ou encore les menaces internes.

Les validations terrain réalisées dans le cadre de cette recherche ont également permis d'observer que plusieurs mesures de sécurité techniquement adéquates perdaient une partie importante de leur efficacité lorsque les procédures, la formation ou la sensibilisation des utilisateurs demeuraient insuffisantes. Ces constats renforcent ainsi la pertinence d'une approche multidimensionnelle de la sécurité intégrant simultanément les technologies, les processus et le facteur humain.

6.2.5 Valeur de la représentation visuelle

Les résultats du sondage ainsi que les validations terrain réalisées auprès de Bombardier et de SportVAC démontrent un fort consensus concernant la valeur de la représentation visuelle proposée. Les participants ont largement considéré que la représentation matricielle facilitait la compréhension globale de la posture de sécurité, permettait d'identifier rapidement certaines forces et faiblesses organisationnelles ainsi que de mieux visualiser les déséquilibres entre les différentes dimensions de sécurité.

Cette capacité de représentation synthétique apparaît particulièrement pertinente dans les contextes organisationnels où les gestionnaires ne possèdent pas nécessairement une expertise approfondie dans l'ensemble des domaines de sécurité. Les validations réalisées suggèrent que l'outil proposé facilite les échanges entre différents intervenants ainsi que les discussions

stratégiques liées à la priorisation des mesures de sécurité. Les résultats obtenus tendent également à démontrer que la représentation visuelle contribue à rendre plus accessibles certaines interactions complexes entre les fonctions de sécurité, les mesures organisationnelles et les différents domaines de protection.

6.3 Contribution de la méthode proposée

Au-delà des constats observés concernant les pratiques actuelles de sécurité, cette recherche visait également à développer un cadre d'analyse permettant d'intégrer différentes dimensions de la sécurité organisationnelle au sein d'une représentation commune. Les validations réalisées permettent d'identifier plusieurs contributions conceptuelles, méthodologiques et pratiques associées à la méthode proposée.

6.3.1 Contribution conceptuelle

L'une des principales contributions conceptuelles de cette recherche réside dans la proposition d'un cadre d'analyse structurant permettant d'intégrer simultanément plusieurs domaines de sécurité généralement abordés de manière distincte dans la littérature et dans les pratiques organisationnelles. La méthode développée repose notamment sur l'intégration de la cybersécurité, de la sécurité physique, de la sécurité de l'information ainsi que du filtrage de sécurité à l'intérieur d'une même architecture d'analyse. Cette approche vise à favoriser une compréhension plus globale des interactions entre les différentes dimensions de sécurité organisationnelle.

La méthode proposée introduit également une structuration basée sur quatre fonctions de sécurité, soit empêcher, détecter, retarder et répondre, combinées à trois axes d'intervention, soit les technologies, les équipements et les services, les procédures ainsi que le facteur humain. Cette représentation permet d'observer certains déséquilibres organisationnels qui demeurent souvent difficiles à visualiser dans les approches traditionnelles de sécurité.

6.3.2 Contribution méthodologique

La présente recherche contribue également au développement d'une approche méthodologique permettant de structurer l'analyse de la sécurité organisationnelle selon une logique multidimensionnelle et visuelle. Contrairement à plusieurs approches principalement orientées vers la conformité normative ou l'évaluation probabiliste des risques, la méthode proposée vise principalement à identifier les déséquilibres, les angles morts et les incohérences organisationnelles entre les différentes fonctions et dimensions de sécurité.

Les validations réalisées suggèrent que cette représentation facilite l'interprétation des résultats, les discussions interdisciplinaires ainsi que l'identification rapide de certaines vulnérabilités organisationnelles. La méthode développée ne vise toutefois pas à remplacer les analyses de risques, les audits de conformité ou les cadres normatifs existants. Elle cherche plutôt à offrir un outil complémentaire permettant d'obtenir une lecture plus globale et structurée de la posture de sécurité organisationnelle.

6.3.3 Contribution pratique pour les PME

Les résultats obtenus dans le cadre de cette recherche suggèrent également que la méthode proposée présente un intérêt particulier pour les petites et moyennes entreprises. Plusieurs cadres normatifs et méthodologies existants apparaissent difficilement applicables dans les PME en raison de leur complexité, des ressources nécessaires à leur implantation ou du niveau élevé d'expertise requis pour leur utilisation.

À l'inverse, la méthode développée dans le cadre de cette recherche vise à offrir une approche plus accessible permettant à des gestionnaires ou à des responsables de sécurité de visualiser rapidement certaines forces, faiblesses et asymétries organisationnelles sans nécessairement devoir réaliser une analyse technique exhaustive. Les validations réalisées tendent également à démontrer que la représentation visuelle proposée facilite les échanges stratégiques entre différents intervenants et peut contribuer à améliorer la compréhension globale des enjeux de sécurité à l'intérieur des organisations.

6.4 Limites de la recherche

Malgré les constats observés et les validations réalisées dans le cadre de cette recherche, certaines limites méthodologiques et opérationnelles doivent être considérées dans l'interprétation des résultats obtenus.

6.4.1 Limites méthodologiques

La présente recherche repose principalement sur une démarche qualitative et exploratoire orientée vers le développement et la validation d'un cadre d'analyse appliqué. Elle ne vise donc pas à produire une modélisation statistique généralisable à l'ensemble des organisations. Les validations réalisées reposent également sur un nombre limité de cas pratiques ainsi que sur un échantillon restreint de répondants provenant majoritairement de milieux professionnels liés à la sécurité. Les résultats obtenus doivent donc être interprétés comme des tendances exploratoires plutôt que comme des conclusions universelles applicables à toutes les organisations.

6.4.2 Limites statistiques

L'analyse des correspondances multiples et la classification ascendante hiérarchique réalisées dans le cadre de cette recherche demeurent de nature exploratoire. La taille relativement limitée de l'échantillon ainsi que certaines concentrations de profils professionnels peuvent influencer les regroupements observés ainsi que l'interprétation des résultats. Les analyses statistiques réalisées avaient principalement pour objectif de soutenir l'interprétation des perceptions recueillies et non de produire une validation quantitative exhaustive de la méthode proposée.

6.4.3 Limites opérationnelles

Certaines limites opérationnelles ont également été observées durant les validations terrain réalisées dans le cadre de cette recherche. Dans plusieurs cas, les gestionnaires interrogés ne possédaient pas nécessairement l'ensemble des informations requises pour répondre avec précision à certaines questions liées à la sécurité organisationnelle. La classification des contrôles à l'intérieur des douze catégories de la matrice a également représenté un défi important dans certains contextes organisationnels, particulièrement lorsque certains contrôles possédaient simultanément plusieurs fonctions ou plusieurs dimensions.

Enfin, les validations réalisées ont mis en évidence l'importance d'utiliser un langage adapté au niveau de compréhension des différents gestionnaires afin d'assurer une interprétation cohérente des questions et des résultats.

6.5 Perspectives futures

Les résultats obtenus dans le cadre de cette recherche ouvrent plusieurs perspectives de développement et d'amélioration futures concernant l'évolution de la méthode proposée ainsi que son application dans différents contextes organisationnels.

6.5.1 Développement logiciel et automatisation

L'une des principales perspectives futures concerne le développement d'une plateforme logicielle permettant d'automatiser partiellement l'analyse des contrôles de sécurité ainsi que la génération des représentations visuelles associées à la méthode proposée. Une telle approche pourrait faciliter l'utilisation de la méthode dans différents contextes organisationnels et permettre une standardisation accrue des analyses réalisées.

6.5.2 Structuration des référentiels

Les travaux réalisés dans le cadre de cette recherche ont également mis en évidence la difficulté d'identifier et de classifier uniformément certains contrôles de sécurité à travers les différents domaines analysés. Des travaux futurs pourraient ainsi viser le développement de référentiels structurés permettant d'associer plus systématiquement certains contrôles aux différentes fonctions et dimensions de sécurité utilisées dans le cadre de la méthode proposée.

6.5.3 Validation élargie

Des validations supplémentaires réalisées auprès d'un plus grand nombre d'organisations provenant de secteurs d'activité variés permettraient également de renforcer la compréhension des déséquilibres organisationnels observés ainsi que la portée pratique de la méthode proposée. Des recherches futures pourraient notamment permettre d'évaluer l'utilisation de la méthode dans différents contextes industriels, gouvernementaux ou critiques.

6.5.4 Utilisation pédagogique et stratégique

Les validations réalisées suggèrent également que la méthode proposée pourrait présenter un intérêt pédagogique important dans les domaines de la formation, de la sensibilisation et du développement des compétences en sécurité. La représentation visuelle développée pourrait notamment être utilisée afin de faciliter la compréhension des interactions entre les différentes dimensions de la sécurité ainsi que pour soutenir certaines discussions stratégiques liées à la gouvernance organisationnelle de la sécurité.

CONCLUSION

La présente recherche visait à développer un cadre d'analyse permettant d'intégrer différentes dimensions de la sécurité organisationnelle à l'intérieur d'une représentation commune et structurée. Plus spécifiquement, cette démarche cherchait à répondre à une problématique fréquemment observée dans les organisations, soit la fragmentation des approches de sécurité ainsi que les déséquilibres existants entre les différentes fonctions et dimensions de protection.

La revue de littérature réalisée dans le cadre de cette recherche a permis de mettre en évidence plusieurs constats importants concernant l'évolution contemporaine des pratiques de sécurité. Les travaux recensés démontrent notamment que la sécurité de l'information demeure encore fréquemment assimilée à la cybersécurité, malgré le fait que la protection de l'information dépasse largement les seules dimensions numériques. La littérature met également en évidence la présence de nombreuses approches normatives, méthodologiques et disciplinaires développées de manière relativement indépendante, particulièrement entre la cybersécurité, la sécurité physique et les approches liées au facteur humain et au filtrage de sécurité.

Les validations terrain réalisées dans le cadre de cette recherche ainsi que les résultats du sondage effectué auprès de professionnels de la sécurité tendent également à démontrer que plusieurs organisations présentent des déséquilibres importants dans leur posture de sécurité. Les résultats obtenus suggèrent notamment une forte concentration des efforts sur les mesures préventives et technologiques, alors que les fonctions détecter, retarder et répondre apparaissent souvent moins développées ou moins structurées. Les analyses réalisées mettent également en évidence des difficultés persistantes d'intégration entre les différents domaines de sécurité ainsi qu'une compréhension parfois limitée des interactions existantes entre les dimensions technologiques, humaines et organisationnelles.

L'analyse exploratoire des données recueillies à l'aide d'une analyse des correspondances multiples et d'une classification ascendante hiérarchique a également permis d'identifier certains regroupements de perception cohérents avec les constats observés durant les

validations terrain. Les résultats obtenus suggèrent notamment l'existence de visions parfois opposées concernant l'intégration de la sécurité, l'équilibre des ressources organisationnelles ainsi que l'importance relative des différentes dimensions de sécurité. Ces observations tendent à démontrer que les difficultés d'intégration observées ne reposent pas uniquement sur des enjeux technologiques, mais également sur des différences conceptuelles, culturelles et disciplinaires entre les domaines de sécurité eux-mêmes.

Dans ce contexte, la principale contribution de cette recherche réside dans le développement d'un cadre d'analyse multidimensionnel permettant de structurer l'évaluation de la sécurité selon quatre fonctions de sécurité, soit empêcher, détecter, retarder et répondre, combinées à trois axes d'intervention, soit les technologies et équipements, les procédures ainsi que le facteur humain. Cette approche vise principalement à faciliter l'identification des déséquilibres organisationnels, des angles morts et des incohérences pouvant exister entre les différentes dimensions de sécurité.

Les validations réalisées dans le cadre de cette recherche suggèrent également que la représentation visuelle proposée constitue l'une des principales forces de la méthode développée. Les participants aux validations terrain ainsi que les répondants du sondage ont largement considéré que la représentation matricielle facilitait la compréhension globale de la posture de sécurité, permettait d'identifier rapidement certaines forces et faiblesses organisationnelles ainsi que de mieux visualiser les déséquilibres entre les différentes dimensions de sécurité. Ces résultats tendent également à démontrer que la méthode proposée peut contribuer à faciliter les discussions interdisciplinaires et à améliorer la compréhension stratégique des enjeux de sécurité organisationnelle.

La présente recherche comporte néanmoins certaines limites. La démarche adoptée demeure principalement qualitative et exploratoire, et les validations réalisées reposent sur un nombre limité de cas pratiques ainsi que sur un échantillon restreint de répondants. Les résultats obtenus doivent donc être interprétés comme des tendances exploratoires plutôt que comme des conclusions universelles applicables à l'ensemble des organisations. De plus, la

classification des contrôles à l'intérieur des différentes catégories de la matrice a parfois représenté un défi important, particulièrement dans les contextes où certains contrôles possédaient simultanément plusieurs fonctions ou dimensions.

Malgré ces limites, les résultats obtenus suggèrent que la méthode développée dans le cadre de cette recherche présente un potentiel intéressant pour les organisations souhaitant améliorer leur compréhension globale de la sécurité. Les perspectives futures associées à cette recherche pourraient notamment inclure le développement d'outils logiciels facilitant l'automatisation des analyses, la création de référentiels structurés de contrôles de sécurité, l'élargissement des validations à différents secteurs d'activité ainsi que l'utilisation de la méthode dans des contextes pédagogiques, stratégiques ou de gouvernance organisationnelle.

Finalement, cette recherche tend à démontrer que le principal défi des organisations contemporaines ne réside pas nécessairement dans l'absence de mesures de sécurité, mais plutôt dans le manque d'équilibre, d'intégration et de cohérence entre les différentes dimensions de la sécurité organisationnelle. Les résultats obtenus suggèrent ainsi qu'une approche multidimensionnelle, structurée et visuelle de la sécurité peut contribuer à améliorer la compréhension globale des enjeux de protection des personnes, des infrastructures et de l'information au sein des organisations modernes.

ANNEXE I

GUIDE D'ENTREVUE UTILISÉ DANS LE CADRE DES ENTREVUES D'EXPERTS

Cette annexe présente le guide d'entrevue semi-dirigée utilisé dans le cadre des entrevues réalisées auprès de professionnels des domaines de la cybersécurité, de la sécurité physique, de la sécurité de l'information et du filtrage de sécurité.

I.1 Consentement et informations générales

Cette entrevue sera enregistrée en format audio et non prise en note écrite. L'objectif est de faciliter l'analyse et la retranscription fidèle des propos. Certaines réponses pourront être citées textuellement dans le mémoire, accompagnées du nom et du titre du participant, sauf indication contraire de sa part. Aucune information ne sera diffusée en dehors de ce cadre académique sans autorisation explicite.

0. Acceptez-vous ces conditions?

□ Oui
□ Non
Date : _____
Heure : _____
Nom du participant : _____
Titre ou fonction : _____
Domaine principal d'expertise : _____

I.2 Questions d'entrevue

I.2.1 Introduction

1. Parlez-nous de vous. Pourquoi êtes-vous considéré comme un acteur reconnu de la sécurité au Québec?

I.2.2 Vision globale et gouvernance

2. Comment définissez-vous la sécurité dans une organisation, au sens large?
3. Parlez-nous de la gouvernance de la sécurité dans les organisations que vous avez connues. Quel rôle joue concrètement le CSO ou le CISO, et est-ce le bon?
4. Voyez-vous souvent des problèmes liés au travail en silos dans les structures de sécurité?

I.2.3 Objectifs et leviers de sécurité

5. Comment les organisations répartissent-elles leurs efforts entre empêcher, détecter, retarder et répondre?
6. Est-ce que cette répartition vous semble équilibrée?
7. Pour atteindre ces objectifs, on peut intervenir sur trois composantes : la technologie, les procédures et le facteur humain. Ces leviers sont-ils exploités de façon équilibrée selon vous?

I.2.4 Normes, outils et PME

8. Quelles sont les principales normes, méthodes ou bonnes pratiques que vous appliquez ou recommandez dans votre domaine?
9. Selon vous, existe-t-il une norme ou un outil qui permet d'évaluer la sécurité d'une PME de manière réellement globale?
10. Qu'est-ce qui empêche, selon vous, les PME d'adopter une approche de sécurité plus structurée et complète?

I.2.5 Facteurs humains et perspectives d'amélioration

11. Quel rôle joue la formation, la sensibilisation et le comportement humain dans l'efficacité réelle des dispositifs de sécurité?
12. À quoi devrait ressembler un bon outil d'évaluation de la sécurité pour les PME?
13. Si vous deviez conseiller une PME qui commence à structurer sa sécurité, quelle serait votre première recommandation?

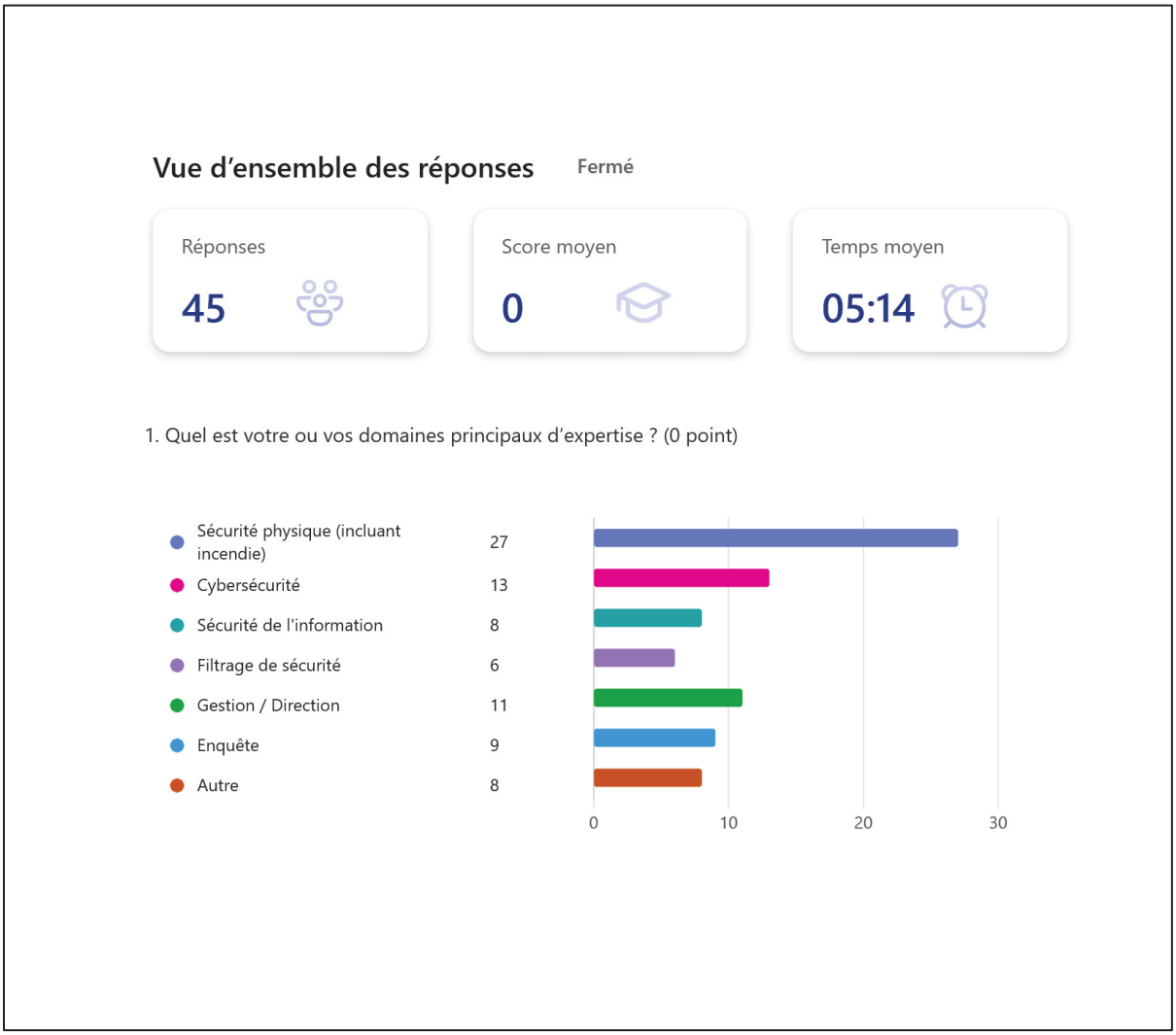
I.2.6 Conclusion

14. Y a-t-il un angle ou un aspect de la sécurité qu'on néglige trop souvent selon vous?

ANNEXE II

QUESTIONNAIRE ET RÉSULTATS SOMMAIRES DU SONDAGE DE VALIDATION

Cette annexe présente le questionnaire utilisé dans le cadre du sondage de validation réalisé auprès des professionnels de la sécurité ainsi qu'un résumé visuel des réponses obtenu à partir de Microsoft Forms.



2. Si vous avez sélectionné “Autre”, veuillez préciser : (0 point)

7
Réponses

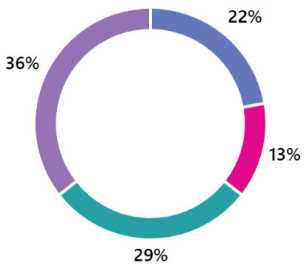
Dernières réponses
...

1 répondants (14%) répondu nouveau type pour cette question.

chiffrement
Media
Renseignement
nouveau type
Certification
Architecture TI
Ventes

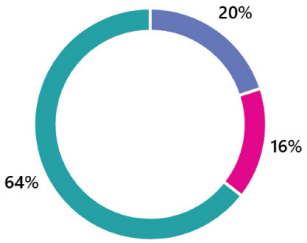
3. Nombre d’années d’expérience en sécurité ou domaine connexe : (0 point)

0 à 5 ans	10
5 à 10 ans	6
10 à 20 ans	13
plus de 20 ans	16

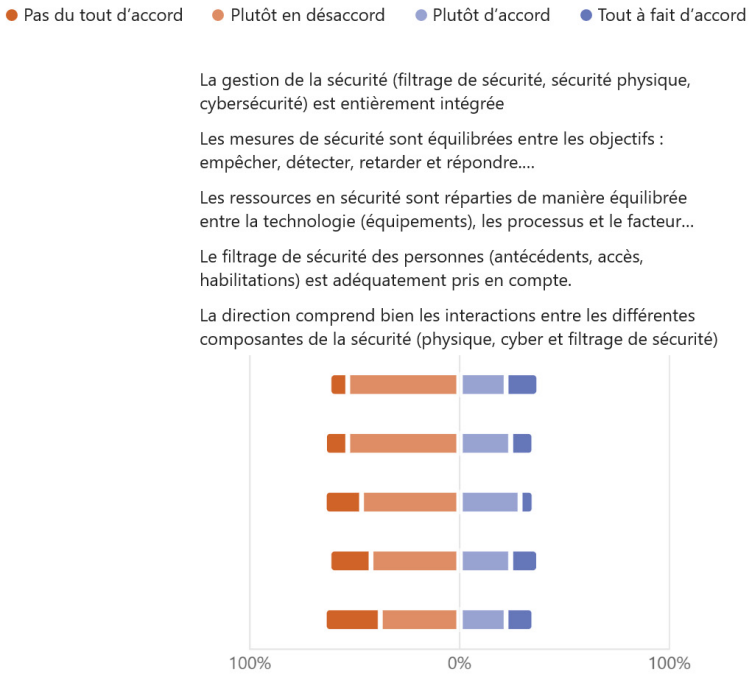


4. Lorsque vous répondez à ce questionnaire, vous vous basez principalement sur : (0 point)

Votre organisation actuelle	9
Plusieurs organisations (expérience de consultation ou multi-clients)	7
Votre expérience globale (carrière)	29



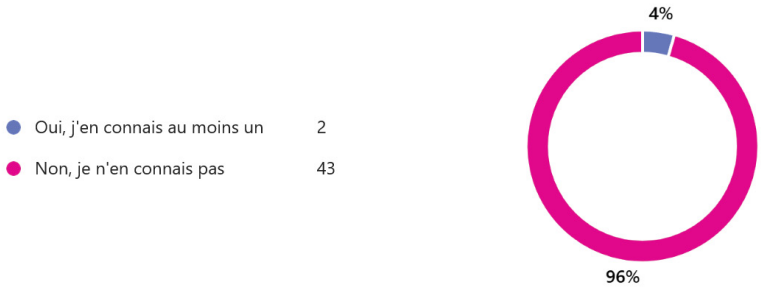
5. Selon votre expérience, au sein de votre organisation ou des organisations avec lesquelles vous travai llez. (0 point)



6. À votre connaissance, existe-t-il un outil d'analyse globale de la posture de sécurité qui :

- intègre sur le même pied d'égalité la sécurité physique, la cybersécurité et le facteur humain (fi ltrage des personnes)
- est accessible ($) et applicable aux PME

(0 point)

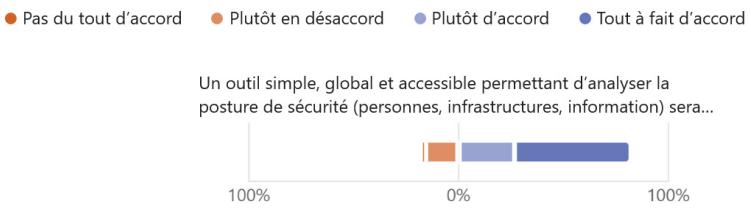


7. Si oui, lequel ? (0 point)

2
Réponses

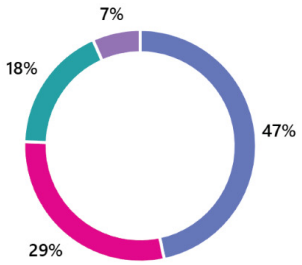
Dernières réponses

8. Indépendamment des outils existants, dans votre pratique : (0 point)



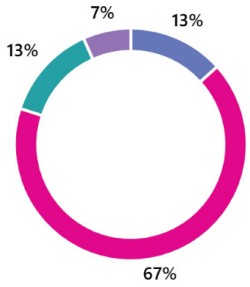
9. Dans votre expérience, quel domaine de la sécurité est le plus négligé dans les organisations ? (0 poi nt)

Le filtrage de sécurité (sélection, vérification, antécédents)	21
La sécurité physique (contrôle d'accès, surveillance, infrastructures, serrurerie, caméras)	13
La cybersécurité (systèmes, réseaux, données)	8
Aucun, les domaines sont généralement équilibrés	3

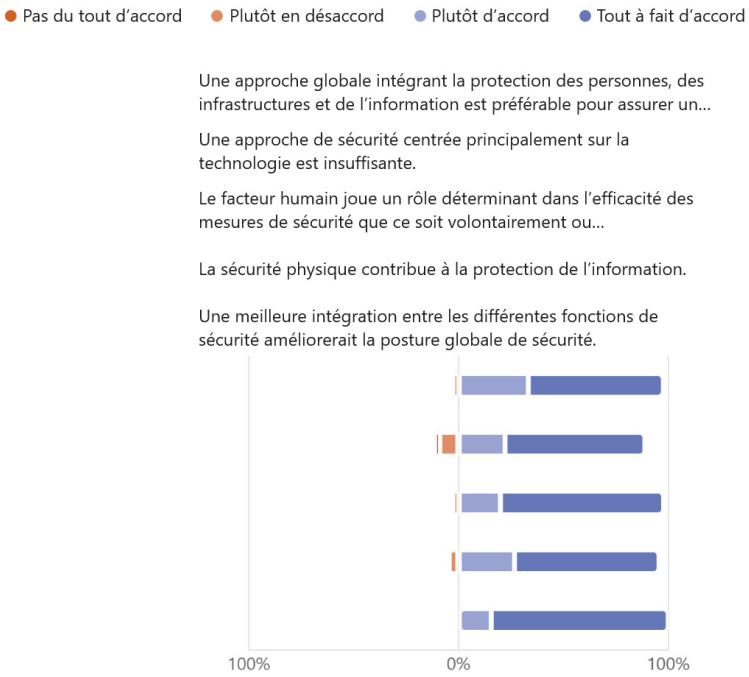


10. Dans votre expérience, les organisations sont suffisamment préparées à détecter une situation anor male et à intervenir efficacement **avant qu'un incident de sécurité n'entraîne une compromissio n des actifs**. (0 point)

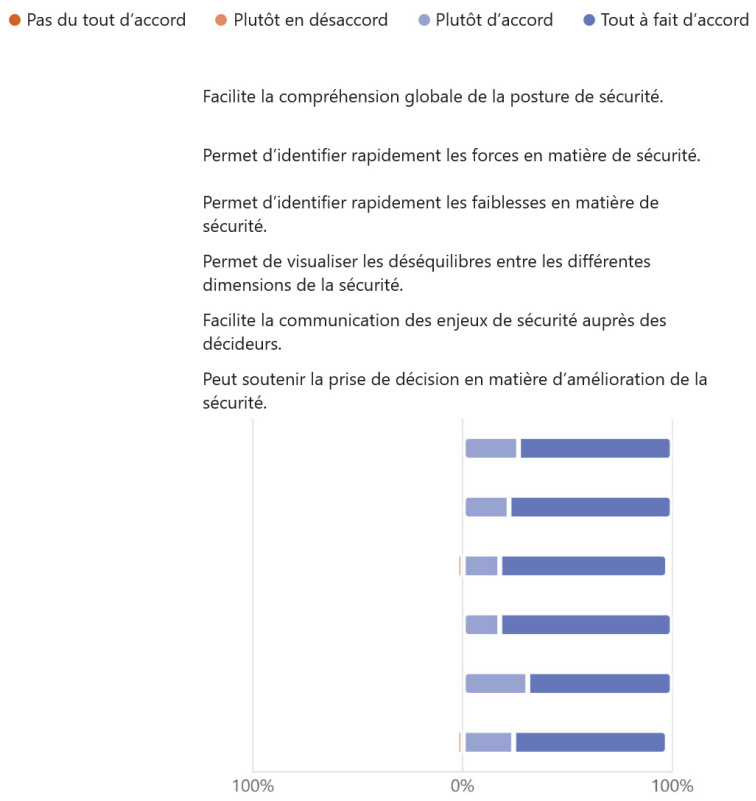
Pas du tout d'accord	6
Plutôt en désaccord	30
Plutôt d'accord	6
Tout à fait d'accord	3



11. Selon votre expérience : (0 point)



12. Selon votre expérience, le modèle présenté ce soir (matrice 4x3 en couleurs) : (0 point)



LISTE DE RÉFÉRENCES BIBLIOGRAPHIQUES

AICPA & CIMA. [s d]. « System and Organization Controls: SOC Suite of Services ». <https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services>. Consulté le 26 mai 2026.

Alexei, Arina et Anatolie Alexei. 2023. « THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY ». *Journal of Engineering Science*, vol. 29, nº 4, p. 72-83. <https://doi.org/10.52326/jes.utm.2022.29(4).08>.

Ambreen, Lubna, Manjula Jain, Rakesh Kumar Yadav et Shweta Loonkar. 2024. « Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review ». *Multidisciplinary Reviews*, vol. 6, p. 2023ss080. <https://doi.org/10.31893/multirev.2023ss080>.

Amsel, E. et T. Amsel. 1989. « Security personnel screening ». In *International Carnahan Conference on Security Technology*. (1989), p. 313-314. IEEE. <https://doi.org/10.1109/CCST.1989.752000>. Consulté le 25 mai 2026.

Anthony (Tony)Cox, Louis. 2008. « What's Wrong with Risk Matrices? » *Risk Analysis*, vol. 28, nº 2, p. 497-512. <https://doi.org/10.1111/j.1539-6924.2008.01030.x>.

ASIS International. 2021. *Protection of Assets (2021 edition) - Physical Security*. 643 p.

ASIS International. 2023. *Implementing Physical Protection Systems: A Practical Guide, 3rd Edition*. ASIS International.

Aubert, Maxime, Rustan Lebe, Adhi Agus Oktaviana, Muhammad Tang, Basran Burhan, Hamrullah, Andi Jusdi, Abdullah, Budianto Hakim, Jian-xin Zhao, I. Made Geria, Priyatno Hadi Sulistyarto, Ratno Sardi et Adam Brumm. 2019. « Earliest hunting scene in prehistoric art ». *Nature*, vol. 576, nº 7787, p. 442-445. <https://doi.org/10.1038/s41586-019-1806-y>.

Aven, Terje. 2016. « Risk assessment and risk management: Review of recent advances on their foundation ». *European Journal of Operational Research*, vol. 253, nº 1, p. 1-13. <https://doi.org/10.1016/j.ejor.2015.12.023>.

Bingley, William J., Katharine H. Greenaway et S. Alexander Haslam. 2022. « A Social-Identity Theory of Information-Access Regulation (SITIAR): Understanding the Psychology of Sharing and Withholding ». *Perspectives on Psychological Science*, vol. 17, nº 3, p. 827-840. <https://doi.org/10.1177/1745691621997144>.

Bowles, Samuel et Herbert Gintis. 2004. « Persistent parochialism: trust and exclusion in ethnic networks ». *Journal of Economic Behavior & Organization*, vol. 55, nº 1, p. 1-23. <https://doi.org/10.1016/j.jebo.2003.06.005>.

Canada, Communications Security Establishment. 2022. « Canadian Centre for Cyber Security ». In *Canadian Centre for Cyber Security*. <https://www.cyber.gc.ca/en>. Consulté le 26 mai 2026.

Center for Internet Security. [s d]. « CIS Controls Version 8 ». In *CIS*. <https://www.cisecurity.org/controls/v8/>. Consulté le 26 mai 2026.

Chen, Cheng. 2024. « Reveal the Evolutionary Trajectory of Digital Innovation in Small and Medium-sized Enterprises ». *Highlights in Business, Economics and Management*, vol. 29, p. 7-16. <https://doi.org/10.54097/dsyj7862>.

Chen, Tsuiping. 2016. « Technology-supported peer feedback in ESL/EFL writing classes: a research synthesis ». *Computer Assisted Language Learning*, vol. 29, nº 2, p. 365-397. <https://doi.org/10.1080/09588221.2014.960942>.

Coles-Kemp, Lizzie. 2009. « Information security management: An entangled research challenge ». *Information Security Technical Report*, vol. 14, nº 4, p. 181-185. <https://doi.org/10.1016/j.istr.2010.04.005>.

Colwill, Carl. 2009. « Human factors in information security: The insider threat – Who can you trust these days? » *Information Security Technical Report*, vol. 14, nº 4, p. 186-196. <https://doi.org/10.1016/j.istr.2010.04.004>.

Crowe, Timothy D. 2000. *Crime prevention through environmental design: applications of architectural design and space management concepts*, 2. ed. Boston, Mass : Butterworth-Heinemann, 333 p.

CST et GRC. 2007. *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)*. <https://www.cyber.gc.ca/sites/default/files/cyber/publications/tra-emr-1-f.pdf>. Consulté le 25 mai 2026.

Da Silva, Joseph et Rikke Bjerg Jensen. 2022. « “Cyber security is a dark art”: The CISO as Soothsayer ». *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, nº CSCW2, p. 1-31. <https://doi.org/10.1145/3555090>.

De Matteis, Jacopo, Gianluca Elia et Pasquale Del Vecchio. 2023. « Business continuity management and organizational resilience: A small and medium enterprises (SMEs) perspective ». *Journal of Contingencies and Crisis Management*, vol. 31, nº 4, p. 670-682. <https://doi.org/10.1111/1468-5973.12470>.

DeConick, April D. 2022. « Keeping Secrets: The Social Practice of Gnostic Secrecy ». In *The Routledge Handbook of Religion and Secrecy*, 1re éd., p. 131-150. London : Routledge. <https://doi.org/10.4324/9781003014751-12>. Consulté le 30 janvier 2026.

Djenna, Amir, Saad Harous et Djamel Eddine Saidouni. 2021. « Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure ». *Applied Sciences*, vol. 11, nº 10, p. 4580. <https://doi.org/10.3390/app11104580>.

Dunn Cavelty, Myriam. 2009. *Cyber-security and threat politics: US efforts to secure the information age*, Transferred to digital print. Coll. « CSS studies in security and international relations ». London : Routledge, 182 p.

Erickson, Bonnie H. 1981. « Secret Societies and Social Structure ». *Social Forces*, vol. 60, nº 1, p. 188. <https://doi.org/10.2307/2577940>.

Etymonline. [s d]. « Security - Etymology, Origin & Meaning ». In *etymonline*. <https://www.etymonline.com/word/security>. Consulté le 4 février 2026.

Garcia, Mary Lynn. 2008. *The design and evaluation of physical protection systems*, 2nd ed. Burlington, MA : Elsevier/Butterworth-Heinemann, 1 p.

Greitzer, Frank L. et Deborah A. Frincke. 2010. « Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation ». In *Insider Threats in Cyber Security*, sous la dir. de Probst, Christian W., Jeffrey Hunker, Dieter Gollmann et Matt Bishop, p. 85-113. Coll. « Advances in Information Security », vol. 49. Boston, MA : Springer US. <https://doi.org/10.1007/978-1-4419-7133-3_5>. Consulté le 25 mai 2026.

Grigaliūnas, Šarūnas, Michael Schmidt, Rasa Brūzgienė, Panayiota Smyrli, Stephanos Andreou et Audrius Lopata. 2024. « Holistic Information Security Management and Compliance Framework ». *Electronics*, vol. 13, nº 19, p. 3955. <https://doi.org/10.3390/electronics13193955>.

Guasch, Teresa, Anna Espasa, Ibis M. Alvarez et Paul A. Kirschner. 2013. « Effects of feedback on collaborative writing in an online learning environment ». *Distance Education*, vol. 34, nº 3, p. 324-338. <https://doi.org/10.1080/01587919.2013.835772>.

Ijiga, Matthew Onuh, Hamed Salam Olarinoye, Francis Asare Baffour Yeboah et Joy Nnenna Okolo. 2025. « Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches ». *International Journal of Scientific Research and Modern Technology*, p. 1-15. <https://doi.org/10.38124/ijsrmt.v4i3.376>.

Innovation, Sciences et Développement économique Canada, De : 2025. « Principales statistiques relatives aux petites entreprises 2024 ». <https://ised-isde.canada.ca/site/recherche-statistique-pme/fr/principales-statistiques-relatives-aux-petites-entreprises/principales-statistiques-relatives-aux-petites-entreprises-2024>. Consulté le 5 février 2026.

International Organization for Standardization. 2018. *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Geneva, Switzerland : ISO.

ISACA. [s d]. « COBIT®| Control Objectives for Information Technologies® ». In *ISACA*. <https://www.isaca.org/resources/cobit>. Consulté le 26 mai 2026.

ISO/IEC. 2018. *Management du risque*.

ISO/IEC. 2019. *Continuité d'activité*.

ISO/IEC. 2022a. *Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information*.

ISO/IEC. 2022b. *Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information*.

Isparta University of Applied Sciences, Department of Information Security, Isparta, Turkey et Ahmet Ali Süzen. 2020. « A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem ». *International Journal of Computer Network and Information Security*, vol. 12, nº 1, p. 1-12. <https://doi.org/10.5815/ijcnis.2020.01.01>.

Karanja, Erastus et Mark A. Rosso. 2017. « The Chief Information Security Officer: An Exploratory Study ». *Journal of International Technology and Information Management*, vol. 26, nº 2, p. 23-47. <https://doi.org/10.58729/1941-6679.1299>.

Kavallieratos, Georgios, Sokratis Katsikas et Vasileios Gkioulos. 2020. « Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey ». *Future Internet*, vol. 12, nº 4, p. 65. <https://doi.org/10.3390/fi12040065>.

Klimburg, Alexander, éd. 2012. *National cyber security framework manual*. Tallinn, Estonia : NATO Cooperative Cyber Defence Centre of Excellence.

Manish Keshavrao Hadap, Arvinder Kour Mehta, Gitti Narsimlu, Parag Jawarkar, Vijay Kumar Kaluvala, et Ajay Kumar Chaturvedi. 2025. « An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs ». *Metallurgical and Materials Engineering*, vol. 31, nº 2, p. 93-97. <https://doi.org/10.63278/1340>.

Melaku, Henock Mulugeta. 2023. « A Dynamic and Adaptive Cybersecurity Governance Framework ». *Journal of Cybersecurity and Privacy*, vol. 3, nº 3, p. 327-350. <https://doi.org/10.3390/jcp3030017>.

Mohamed, Ihab, Hesham A. Hefny et Nagy R. Darwish. 2024. « Enhancing Cybersecurity Defenses: A Multicriteria Decision-Making Approach to Mitre ATT&CK Mitigation Strategy ». *International journal of Computer Networks & Communications*, vol. 16, nº 4, p. 19-35. <https://doi.org/10.5121/ijcnc.2024.16402>.

National Fire Protection Association. [s d]. « NFPA | The National Fire Protection Association ». <https://www.nfpa.org/en>. Consulté le 26 mai 2026.

Nieles, Michael, Kelley Dempsey et Victoria Yan Pillitteri. 2017. *An introduction to information security*. NIST SP 800-12r1. Gaithersburg, MD : National Institute of Standards and Technology, NIST SP 800-12r1 p. <https://doi.org/10.6028/NIST.SP.800-12r1>. Consulté le 4 février 2026.

NIST. 2013. « Cybersecurity Framework ». *NIST*. <https://www.nist.gov/cyberframework>. Consulté le 26 mai 2026.

NIST - Joint Task Force Transformation Initiative. 2012. *Guide for conducting risk assessments*. NIST SP 800-30r1. Gaithersburg, MD : National Institute of Standards and Technology, NIST SP 800-30r1 p. <https://doi.org/10.6028/NIST.SP.800-30r1>. Consulté le 6 février 2026.

Nowak, Martin A. et David C. Krakauer. 1999. « The evolution of language ». *Proceedings of the National Academy of Sciences*, vol. 96, nº 14, p. 8028-8033. <https://doi.org/10.1073/pnas.96.14.8028>.

Ogunyomi, Paul et Nealia S. Bruning. 2016. « Human resource management and organizational performance of small and medium enterprises (SMEs) in Nigeria ». *The International Journal of Human Resource Management*, vol. 27, nº 6, p. 612-634. <https://doi.org/10.1080/09585192.2015.1033640>.

Pittala, Satish Kumar et Vikram Kumar Casula Ashok. 2023. « A New Era in Security: Bridging Information Security and Cybersecurity ». *International Journal of Multidisciplinary Futuristic Development*, vol. 4, nº 1, p. 69-72. <https://doi.org/10.54660/IJMFD.2023.4.1.69-72>.

Raufi, Basheer Riskhan Abdul Moqset et Muhammad Hamza Usmani. 2024. « Physical Security to Cybersecurity (Challenges and Implications in the Modern Digital Landscape) ». *Journal of Electrical Systems*, vol. 20, nº 4s, p. 692-702. <https://doi.org/10.52783/jes.2090>.

Rushchenko, Julia, Ihor Rushchenko et Olena Plakhova. 2020. « Mitigating hiring risks through pre-employment background screening: Methodology based on the personnel security approach ». *Technium Social Sciences Journal*, vol. 9, p. 577-587. <https://doi.org/10.47577/tssj.v9i1.1109>.

Service canadien du renseignement de sécurité. 2018. « Filtrage de sécurité du gouvernement - Canada.ca ». In *Gouvernement du Canasa*. <https://www.canada.ca/fr/service-renseignement-securite/services/filtrage-de-securite-du-gouvernement.html>. Consulté le 1 juillet 2025.

Taherdoost, Hamed. 2022. « Cybersecurity vs. Information Security ». *Procedia Computer Science*, vol. 215, p. 483-487. <https://doi.org/10.1016/j.procs.2022.12.050>.

Tsvetkov, V. Ya. 2024. « Digital transformation and digital public administration ». *E-Management*, vol. 7, nº 4, p. 69-79. <https://doi.org/10.26425/2658-3445-2024-7-4-69-79>.

U.S. Department of War. [s d]. « CIO - Cybersecurity Maturity Model Certification ». <https://dodcio.defense.gov/CMMC/>. Consulté le 26 mai 2026.

Valladas, H., J. Clottes, J.-M. Geneste, M. A. Garcia, M. Arnold, H. Cachier et N. Tisnérat-Laborde. 2001. « Evolution of prehistoric cave art ». *Nature*, vol. 413, nº 6855, p. 479-479. <https://doi.org/10.1038/35097160>.

Von Solms, Rossouw et Johan Van Niekerk. 2013. « From information security to cyber security ». *Computers & Security*, vol. 38, p. 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>.