INTERNATIONAL JOURNAL OF RESEARCH IN ECONOMICS AND FINANCE, 2026, Vol. 3, No. 6-1, 85-103. https://doi.org/10.71420/ijref.v3i6-1.323

Cybersécurité, gouvernance et performance organisationnelle des PME marocaines : une analyse empirique par la modélisation PLS-SEM

Cybersecurity, governance and organizational performance of Moroccan SMEs: an empirical analysis using PLS-SEM modeling

Ikram BOUABDALLAOUI
Laboratoire Régulations Économiques et Intelligence Stratégique, FSJES Mohammedia, Université Hassan II, Mohammedia, Maroc.

Rhizlane DEFOUAD
Laboratoire Régulations Économiques et Intelligence Stratégique, FSJES Mohammedia, Université Hassan II, Mohammedia, Maroc.

Résumé. La transformation numérique des petites et moyennes entreprises marocaines accroît leur exposition aux risques cybernétiques, tout en soulevant des enjeux majeurs de gouvernance, de transparence informationnelle, de contrôle interne, de responsabilité managériale et de performance organisationnelle. Cette recherche analyse l'impact des pratiques de cybersécurité sur la gouvernance des PME marocaines, en intégrant le rôle médiateur de la culture de cybersécurité organisationnelle et le rôle modérateur du cadre réglementaire et institutionnel perçu. L'originalité de cette étude réside dans la conceptualisation de la cybersécurité non comme un simple dispositif technique, mais comme un levier organisationnel et institutionnel de gouvernance. Sur le plan théorique, l'article articule la théorie de l'agence, la théorie des parties prenantes, la théorie institutionnelle et l'approche par les ressources afin d'expliquer comment les pratiques cybernétiques peuvent réduire les asymétries d'information, renforcer la reddition de comptes et améliorer la qualité des mécanismes de contrôle. Sur le plan méthodologique, l'étude teste un modèle multidimensionnel intégrant cinq dimensions de cybersécurité, quatre dimensions de gouvernance, une variable médiatrice et une variable modératrice dans le contexte spécifique des PME marocaines. Sur le plan managérial, elle propose une hiérarchisation des leviers de cybersécurité les plus pertinents pour les dirigeants de PME. L'étude repose sur une enquête quantitative transversale menée auprès de 246 dirigeants de PME marocaines. Les données ont été traitées selon une démarche séquentielle combinant la purification psychométrique sous SPSS et la modélisation par équations structurelles selon l'approche Partial Least Squares Structural Equation Modeling sous SmartPLS 4, avec bootstrapping de 5 000 sous-échantillons. Les résultats montrent que les pratiques organisationnelles de cybersécurité — politiques et procédures, formation et sensibilisation, conformité réglementaire — produisent des effets significatifs sur la gouvernance, tandis que les technologies de protection et la gestion des incidents ne génèrent pas, à elles seules, d'effets directs significatifs. La culture de cybersécurité joue un rôle médiateur partiel et sélectif, alors que le cadre réglementaire et institutionnel perçu ne présente pas d'effet modérateur significatif. Enfin, la transparence informationnelle, le contrôle interne et la responsabilité des dirigeants contribuent positivement à la performance organisationnelle.
Mots-clés : *cybersécurité ; gouvernance des PME ; performance organisationnelle ; culture de cybersécurité ; cadre réglementaire ; PLS-SEM ; Maroc.*

Abstract. The digital transformation of Moroccan small and medium-sized enterprises (SMEs) increases their exposure to cyber risks, while also raising major issues related to governance, information transparency, internal control, managerial accountability, and organizational

performance. This research analyzes the impact of cybersecurity practices on the governance of Moroccan SMEs, integrating the mediating role of organizational cybersecurity culture and the moderating role of the perceived regulatory and institutional framework. The originality of this study lies in its conceptualization of cybersecurity not as a simple technical device, but as an organizational and institutional lever for governance. Theoretically, the article combines agency theory, stakeholder theory, institutional theory, and the resource-based view to explain how cybersecurity practices can reduce information asymmetries, strengthen accountability, and improve the quality of control mechanisms. Methodologically, the study tests a multidimensional model integrating five cybersecurity dimensions, four governance dimensions, a mediating variable, and a moderating variable within the specific context of Moroccan SMEs. From a managerial perspective, it proposes a ranking of the most relevant cybersecurity levers for SME leaders. The study is based on a cross-sectional quantitative survey conducted with 246 Moroccan SME leaders. The data were processed using a sequential approach combining psychometric purification with SPSS and structural equation modeling using the Partial Least Squares Structural Equation Modeling approach with SmartPLS 4, with bootstrapping of 5,000 subsamples. The results show that organizational cybersecurity practices—policies and procedures, training and awareness, and regulatory compliance—have significant effects on governance, while protection technologies and incident management alone do not generate significant direct effects. Cybersecurity culture plays a partial and selective mediating role, while the perceived regulatory and institutional framework does not have a significant moderating effect. Finally, information transparency, internal controls, and leadership accountability contribute positively to organizational performance.

Keywords: *cybersecurity; SME governance; organizational performance; cybersecurity culture; regulatory framework; PLS-SEM; Morocco*.

1. Introduction

La transformation numérique des entreprises a profondément modifié les conditions d'exercice de l'activité économique. Pour les PME, cette transformation se traduit par une double dynamique : d'une part, l'accès à de nouveaux outils de productivité, de commercialisation, de dématérialisation et de coordination ; d'autre part, une exposition croissante à des cybermenaces susceptibles d'affecter la continuité d'activité, la confidentialité des données, la confiance des partenaires et la réputation de l'entreprise. Cette dualité est particulièrement sensible dans les économies émergentes, où la digitalisation progresse rapidement sans toujours s'accompagner d'une maturité équivalente en matière de gouvernance numérique.

Au Maroc, les PME constituent une composante essentielle du tissu économique. Leur compétitivité dépend de plus en plus de leur capacité à adopter les technologies numériques, à sécuriser leurs actifs informationnels et à instaurer des mécanismes de gouvernance adaptés aux risques contemporains. La promulgation de la Loi 05-20 relative à la cybersécurité, la Loi 09-08 relative à la protection des données personnelles, ainsi que le rôle institutionnel de la DGSSI et de la CNDP traduisent une volonté de structuration de l'écosystème national. Toutefois, l'effectivité de ces dispositifs au sein des PME demeure hétérogène, en raison des contraintes budgétaires, du manque de compétences spécialisées et du poids des pratiques informelles de gouvernance.

La littérature internationale sur la cybersécurité s'est longtemps concentrée sur les dimensions techniques de la protection des systèmes d'information : pare-feu, antivirus, sauvegardes, authentification ou contrôle d'accès. Or, cette perspective demeure insuffisante pour saisir les effets organisationnels de la cybersécurité. La sécurité numérique n'est pas seulement une infrastructure

technique ; elle constitue aussi un ensemble de règles, de routines, de responsabilités, de comportements et de mécanismes de contrôle qui transforment la manière dont l'information est produite, vérifiée, partagée et utilisée dans l'organisation. Elle devient ainsi une composante de la gouvernance.

Cette recherche part de la problématique suivante : dans quelle mesure les pratiques de cybersécurité influencent-elles la gouvernance des PME marocaines, et dans quelle mesure cette gouvernance renforcée contribue-t-elle à leur performance organisationnelle ? Cette problématique appelle une lecture intégrative. Elle suppose d'identifier les dimensions de cybersécurité les plus déterminantes, d'examiner le rôle de la culture organisationnelle comme mécanisme de transmission, d'évaluer l'effet conditionnel du cadre réglementaire et de vérifier si les améliorations de gouvernance se traduisent effectivement par des gains de performance.

L'article poursuit quatre objectifs principaux. Le premier est de proposer un cadre conceptuel reliant les pratiques de cybersécurité à la gouvernance des PME marocaines. Le deuxième est de tester empiriquement les effets directs de cinq dimensions de cybersécurité — politiques et procédures, technologies et infrastructures, formation et sensibilisation, gestion des incidents et continuité d'activité, conformité réglementaire — sur quatre dimensions de gouvernance. Le troisième est d'examiner le rôle médiateur de la culture de cybersécurité et le rôle modérateur du cadre réglementaire et institutionnel perçu. Le quatrième est d'analyser la contribution de la gouvernance à la performance organisationnelle.

La contribution de l'article est triple. Sur le plan théorique, il articule plusieurs cadres analytiques — théorie de l'agence, théorie des parties prenantes, théorie institutionnelle, théorie des ressources et des capacités dynamiques, théorie du signal et théories comportementales de l'adoption technologique — afin de conceptualiser la cybersécurité comme un levier de gouvernance. Sur le plan méthodologique, il mobilise la PLS-SEM pour tester un modèle multidimensionnel adapté aux phénomènes organisationnels complexes. Sur le plan managérial, il propose une hiérarchie opérationnelle des leviers à privilégier par les dirigeants de PME marocaines.

Cette recherche apporte trois contributions principales. Premièrement, sur le plan théorique, elle propose une lecture intégrative de la cybersécurité comme mécanisme de gouvernance des PME, en dépassant l’approche technocentrée dominante. Elle montre que les pratiques de cybersécurité peuvent agir comme des dispositifs de réduction des asymétries d’information, de formalisation des responsabilités, de renforcement du contrôle interne et de construction de la confiance avec les parties prenantes. Deuxièmement, sur le plan méthodologique, l’étude développe et teste empiriquement un modèle multidimensionnel combinant les dimensions organisationnelles, techniques, humaines et institutionnelles de la cybersécurité avec plusieurs dimensions de gouvernance et de performance. L’utilisation de la PLS-SEM permet d’évaluer simultanément les effets directs, indirects et conditionnels, ce qui constitue une contribution adaptée à l’analyse de phénomènes organisationnels complexes. Troisièmement, sur le plan managérial, cette recherche identifie les leviers de cybersécurité les plus structurants pour les PME marocaines et montre que la formalisation des politiques, la formation des collaborateurs et la conformité réglementaire constituent des priorités plus déterminantes que l’investissement technologique isolé.

Le contexte marocain présente des spécificités institutionnelles qui justifient l’analyse de la relation entre cybersécurité et gouvernance des PME. D’une part, la gouvernance des PME marocaines demeure souvent marquée par la concentration du pouvoir décisionnel autour du dirigeant-propriétaire, la prépondérance des relations informelles, la faible séparation entre fonctions de

direction, de contrôle et d'exécution, ainsi que l'absence fréquente de comités spécialisés ou de responsables dédiés à la conformité numérique. D'autre part, les PME évoluent dans un environnement institutionnel en structuration, caractérisé par le renforcement progressif des obligations relatives à la sécurité des systèmes d'information et à la protection des données personnelles. La Loi n° 05-20 fixe notamment le cadre national de gouvernance de la cybersécurité et les règles applicables à certains systèmes d'information, infrastructures et opérateurs, tandis que la Loi n° 09-08 encadre la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Ces spécificités créent une tension entre, d'un côté, des exigences croissantes de conformité, de traçabilité, de contrôle et de responsabilité, et, de l'autre, des capacités organisationnelles souvent limitées au sein des PME. Les contraintes budgétaires, le déficit de compétences spécialisées, la dépendance à des prestataires externes, la faible formalisation des procédures internes et l'hétérogénéité du niveau de maturité numérique peuvent influencer la manière dont les pratiques de cybersécurité se traduisent — ou non — en mécanismes effectifs de gouvernance. Le cas marocain constitue ainsi un terrain pertinent pour examiner si la cybersécurité agit comme un levier réel de gouvernance ou si elle reste limitée à une conformité formelle et technique.

2. Cadre théorique et développement des hypothèses

a. Cybersécurité et gouvernance : une relation multidimensionnelle

La relation entre cybersécurité et gouvernance ne peut être réduite à un lien technique entre protection informatique et maîtrise des risques. Elle engage simultanément des mécanismes d'information, de contrôle, de responsabilité, de conformité et d'apprentissage organisationnel. Dans la perspective de la théorie de l'agence, les pratiques de cybersécurité réduisent les asymétries d'information en imposant des règles de traçabilité, de journalisation, d'autorisation et de reddition de comptes. Elles permettent ainsi aux dirigeants, associés, partenaires et financeurs d'obtenir une information plus fiable sur les processus critiques de l'entreprise.

La théorie des parties prenantes élargit cette lecture en considérant que la PME ne gouverne pas seulement ses relations internes, mais également les attentes de ses clients, fournisseurs, salariés, banques, administrations et partenaires numériques. La protection des données, la continuité du service et la prévention des incidents deviennent des obligations relationnelles qui conditionnent la confiance. La cybersécurité apparaît alors comme un instrument de préservation des intérêts des parties prenantes et de maintien de la légitimité organisationnelle.

La théorie institutionnelle permet de situer les pratiques cybernétiques dans un environnement de règles, de normes et de pressions. Les lois, standards, certifications, recommandations publiques et attentes professionnelles créent des pressions coercitives, normatives et mimétiques qui encouragent les PME à formaliser leurs pratiques. Dans le cas marocain, la Loi 05-20, la Loi 09-08 et l'action des institutions spécialisées constituent un cadre institutionnel en construction, dont l'effectivité dépend de sa compréhension, de sa perception et de son appropriation par les dirigeants.

La théorie des ressources et des capacités dynamiques complète l'analyse en considérant la cybersécurité comme un actif organisationnel. Une PME qui développe des compétences de détection, de prévention, de réponse et d'apprentissage face aux incidents dispose d'une capacité dynamique lui permettant de préserver sa continuité, sa réputation et sa compétitivité. La théorie du signal souligne enfin que les politiques formalisées, les certifications et la conformité peuvent signaler aux partenaires la qualité de la gouvernance et réduire l'incertitude dans les relations d'affaires.

b. Dimensions opérationnelles de la cybersécurité

Dans cette recherche, la cybersécurité est définie comme un construit organisationnel multidimensionnel composé de cinq dimensions complémentaires. Les politiques et procédures (PP) renvoient à l'existence de règles formalisées encadrant l'accès aux systèmes, la gestion des mots de passe, les sauvegardes, la confidentialité et la responsabilité des utilisateurs. Les technologies et infrastructures (TI) couvrent les outils de protection technique tels que les pare-feu, antivirus, authentification, sauvegardes ou systèmes de surveillance. La formation et la sensibilisation (FS) désignent les actions visant à développer les compétences et les réflexes de sécurité des dirigeants et collaborateurs.

La gestion des incidents et la continuité d'activité (GI) renvoient aux procédures de détection, réponse, restauration et apprentissage post-incident. Enfin, la conformité réglementaire et normative (CR) correspond à l'alignement des pratiques internes sur les obligations légales et les standards professionnels applicables. Ces cinq dimensions ne sont pas interchangeables : une PME peut disposer de technologies sans formation, de politiques sans tests d'incidents, ou d'une conformité formelle sans culture partagée. D'où l'intérêt d'une approche dimensionnelle permettant de distinguer leurs contributions respectives à la gouvernance.

c. Gouvernance des PME et performance organisationnelle

La gouvernance des PME présente des spécificités distinctes de celle des grandes entreprises cotées. Elle est fréquemment caractérisée par la concentration du pouvoir décisionnel dans les mains du dirigeant-propriétaire, l'importance des relations informelles, la faiblesse des comités spécialisés et la rareté des fonctions dédiées au contrôle interne ou à la conformité. Dès lors, l'évaluation de la gouvernance ne peut se limiter à la présence de structures formelles ; elle doit porter sur des pratiques observables et adaptées aux PME.

Quatre dimensions sont retenues : la transparence et la communication de l'information (TC), le contrôle interne et les systèmes d'audit (CI), la prise de décision stratégique et le management des risques (PD), ainsi que la responsabilité et la responsabilisation des dirigeants (RA). Ces dimensions permettent d'évaluer la capacité de la PME à produire une information fiable, à contrôler ses processus, à intégrer les risques dans la décision et à rendre compte des responsabilités.

La performance organisationnelle (PO) est appréhendée de manière multidimensionnelle. Elle ne se réduit pas aux résultats financiers immédiats ; elle inclut également la qualité de fonctionnement, la continuité d'activité, la satisfaction des parties prenantes, la réputation, l'efficience et la capacité d'adaptation. Dans cette perspective, une gouvernance renforcée par la cybersécurité devrait contribuer à la performance en réduisant les coûts d'incidents, en améliorant la qualité de l'information et en renforçant la confiance des partenaires.

d. Hypothèses de recherche

Sur la base de ce cadre théorique, neuf hypothèses structurent le modèle conceptuel. Les cinq premières portent sur les effets directs des dimensions de cybersécurité sur la gouvernance ; les deux suivantes portent sur les mécanismes de médiation et de modération ; les deux dernières relient la cybersécurité, la gouvernance et la performance.

Tableau 1 : Hypothèses de recherche

N°	Hypothèse de recherche	Relation	Type / Sens	Ancrage théorique principal
H1	Les politiques et procédures de cybersécurité influencent positivement et significativement la gouvernance des PME marocaines.	PP → GOU	Direct / Positif	Jensen et Meckling (1976) ; Bulgurcu et al. (2010) ; ISO 27001:2022
H2	Les technologies et infrastructures de protection cybernétique influencent positivement et significativement la gouvernance des PME marocaines.	TI → GOU	Direct / Positif	COSO (2013) ; Gordon et al. (2006) ; Barney (1991)
H3	La formation et la sensibilisation à la cybersécurité influencent positivement et significativement la gouvernance des PME marocaines.	FS → GOU	Direct / Positif	Freeman (1984) ; ENISA (2020) ; Davis (1989)
H4	La gestion des incidents de cybersécurité et la continuité d'activité influencent positivement et significativement la gouvernance des PME marocaines.	GI → GOU	Direct / Positif	Monks et Minow (2011) ; Anderson et al. (2019) ; ISO 22301:2019
H5	La conformité réglementaire et normative en matière de cybersécurité influence positivement et significativement la gouvernance des PME marocaines.	CR → GOU	Direct / Positif	DiMaggio et Powell (1983) ; Héroux (2017) ; Spence (1973)
H6	La culture de cybersécurité organisationnelle médiatise positivement et significativement la relation entre les pratiques de cybersécurité et la gouvernance des PME marocaines.	CS → CCO → GOU	Médiateur / Positif	Schlienger et Teufel (2003) ; Da Veiga et al. (2020) ; North (1990)
H7	Le cadre réglementaire et institutionnel modère positivement et significativement la relation entre les pratiques de cybersécurité et la gouvernance des PME marocaines.	CRI × CS → GOU	Modérateur / Positif	DiMaggio et Powell (1983) ; Zolait et al. (2010) ; DGSSI (2022)
H8	La cybersécurité influence positivement et significativement la performance organisationnelle des PME marocaines.	CS → PO	Direct / Positif	Barney (1991) ; Ponemon Institute (2022) ; Anderson et al. (2019)
H9	La gouvernance des PME influence positivement et significativement leur performance organisationnelle.	GOU → PO	Direct / Positif	Brown et Caylor (2006) ; Bebchuk et al. (2009) ; Freeman (1984)

Source : élaboré par nous à partir de la revue de littérature

3. Méthodologie de recherche

a. Design de recherche

La recherche adopte une démarche hypothético-déductive et un design quantitatif transversal par enquête. Ce choix est cohérent avec l'objectif de tester un modèle causal composé de plusieurs construits latents et d'évaluer simultanément des effets directs, indirects et d'interaction. L'approche PLS-SEM est retenue en raison de son adéquation aux modèles prédictifs, aux échantillons de taille moyenne, aux construits multidimensionnels et aux relations complexes incluant médiation et modération.

Le dispositif empirique repose sur un questionnaire bilingue français-arabe administré auprès de dirigeants de PME marocaines. L'unité d'analyse est l'entreprise, appréhendée à travers les réponses du dirigeant ou d'un responsable disposant d'une vision transversale des pratiques de cybersécurité, de gouvernance et de performance.

L'échantillon final retenu pour l'ensemble des analyses statistiques comprend 246 questionnaires valides, ce qui correspond à un taux de réponse net de 70,3 %. Ce taux dépasse significativement les normes habituellement observées dans les enquêtes auto-administrées auprès des PME, généralement comprises entre 20 % et 40 % pour les enquêtes postales et entre 10 % et 30 % pour les enquêtes en ligne non institutionnalisées (Dillman et al., 2014 ; Baruch et Holtom, 2008). Cette performance s'explique par la combinaison de plusieurs facteurs : le caractère institutionnel de la diffusion via les réseaux des CRI et de la CGEM, la garantie d'anonymat clairement formulée dans la lettre d'accompagnement, la pertinence perçue de la thématique cybernétique par les dirigeants dans un contexte post-Loi 05-20, et la disponibilité d'une version bilingue français-arabe du questionnaire qui a réduit la barrière linguistique pour les dirigeants dont le français n'est pas la langue professionnelle principale.

Le questionnaire final est organisé en onze parties thématiques correspondant aux sept construits du modèle et à leurs dimensions, précédées d'une partie introductive sur le profil sociodémographique et organisationnel du répondant. Cette structure suit les recommandations de Dillman, Smyth et Christian (2014) pour la conception de questionnaires optimisant le taux de réponse et la qualité des données collectées, en organisant les items du plus général au plus spécifique et en évitant les transitions abruptes entre thèmes.

b. Échantillon et collecte des données

La population cible de cette recherche est constituée des PME marocaines engagées, à des degrés variables, dans des processus de digitalisation et susceptibles d'être exposées à des risques liés à la sécurité des systèmes d'information, à la protection des données, à la continuité d'activité et à la gouvernance numérique. L'unité d'analyse retenue est l'entreprise, tandis que l'unité de réponse est le dirigeant, le propriétaire-dirigeant, le responsable administratif et financier, le responsable informatique ou tout cadre disposant d'une vision transversale des pratiques de cybersécurité et de gouvernance.

L'étude a mobilisé une méthode d'échantillonnage non probabiliste raisonnée, complétée par une diffusion institutionnelle et professionnelle. Ce choix s'explique par l'absence d'une base de sondage exhaustive et directement accessible recensant les PME marocaines selon leur niveau de maturité cybernétique. Les répondants ont été sollicités à travers des réseaux professionnels, des contacts institutionnels et des canaux numériques, notamment les réseaux liés aux Centres

régionaux d'investissement, aux organisations professionnelles et aux structures d'accompagnement des entreprises.

Les critères d'inclusion étaient les suivants : être une PME localisée au Maroc ; exercer une activité économique formelle ; utiliser des outils numériques dans la gestion, la communication, la relation client, la comptabilité, la production ou la commercialisation ; disposer d'un répondant ayant une connaissance suffisante des pratiques internes de cybersécurité, de gouvernance et de performance ; accepter de participer à l'enquête de manière volontaire et anonyme. Ont été exclus les questionnaires incomplets, incohérents, redondants ou provenant d'organisations ne correspondant pas au profil PME retenu.

La collecte des données s'est déroulée sur une période de cinq mois, du 30 octobre 2025 au 31 mars 2026. Au total, 350 questionnaires ont été distribués ou transmis. Après contrôle de la complétude, de la cohérence interne et du respect des critères d'inclusion, 246 réponses valides ont été retenues pour les analyses statistiques, soit un taux de réponse net de 70,3 %. Ce volume d'observations est compatible avec les exigences de la PLS-SEM et permet de tester un modèle multidimensionnel intégrant des effets directs, médiateurs et modérateurs.

c. Mesure des variables

Les variables ont été mesurées à l'aide d'échelles de Likert en cinq points. Les dimensions de cybersécurité comprennent PP, TI, FS, GI et CR. La gouvernance est mesurée par quatre dimensions : TC, CI, PD et RA. La culture de cybersécurité organisationnelle (CCO) est introduite comme variable médiatrice ; le cadre réglementaire et institutionnel perçu (CRI) comme variable modératrice ; la performance organisationnelle (PO) comme variable dépendante finale.

Les items ont fait l'objet d'une purification psychométrique. Les analyses de fiabilité sous SPSS ont conduit à supprimer certains items présentant des corrélations item-total insuffisantes ou dégradant l'alpha de Cronbach. À titre d'exemple, l'échelle PP présente un alpha de 0,870 après suppression de PP6, et l'échelle TI atteint 0,820 après suppression des items TI5 et TI3. Cette étape a permis de renforcer la cohérence interne des échelles avant l'estimation du modèle PLS-SEM.

Tableau 2 : Critères d'évaluation du modèle PLS-SEM

Critère	Indicateur	Seuil acceptable	Référence
Fiabilité des construits réflexifs	Alpha de Cronbach	≥ 0,70	Nunnally et Bernstein (1994)
	Fiabilité composite (ρc)	≥ 0,70	Hair et al. (2022)
Validité convergente	Outer loadings	≥ 0,70	Hair et al. (2022)
	AVE	≥ 0,50	Fornell et Larcker (1981)
Validité discriminante	HTMT	< 0,85	Henseler et al. (2015)
	Critère Fornell-Larcker	√AVE > corrélations inter-construits	Fornell et Larcker (1981)
Mesure formative (multicolinéarité)	VIF	< 3,3	Hair et al. (2022)
Mesure formative (significativité)	Poids formatifs (p-value)	p < 0,05	Hair et al. (2022)
Pouvoir explicatif	R^2	≥ 0,25 (faible), ≥ 0,50 (modéré), ≥ 0,75 (fort)	Hair et al. (2022)
Taille des effets	f^2	≥ 0,02 (faible), ≥ 0,15 (moyen), ≥ 0,35 (fort)	Cohen (1988)
Pertinence prédictive	Q^2	> 0 (faible), > 0,25 (moyen), > 0,50 (fort)	Hair et al. (2022)
Effets directs	Coefficient de chemin β (t-value)	t > 1,96 (p < 0,05)	Hair et al. (2022)
Médiation	Effet indirect (IC à 95 %)	IC n'incluant pas zéro	Preacher et Hayes (2008)
Modération	Coefficient d'interaction (t-value)	t > 1,96 (p < 0,05)	Henseler et Fassott (2010)

Source : élaboré par nous à partir de la revue de littérature méthodologique

d. Procédure d'analyse

La procédure d'analyse comprend trois étapes. Premièrement, les données ont été décrites et contrôlées afin d'évaluer la qualité de l'échantillon, les distributions et le risque de biais de méthode commune. Deuxièmement, les échelles ont été purifiées par l'analyse de fiabilité et l'analyse factorielle exploratoire. Troisièmement, le modèle de mesure et le modèle structurel ont été estimés sous SmartPLS 4.

Le modèle de mesure a été évalué à travers les charges externes, l'alpha de Cronbach, la fiabilité composite, l'AVE et le critère HTMT. Le modèle structurel a été évalué par les coefficients de chemin, les R^2, les tailles d'effet f^2, la pertinence prédictive Q^2 et les résultats du bootstrapping avec 5 000 sous-échantillons. Les hypothèses ont été considérées comme confirmées lorsque le coefficient était positif, statistiquement significatif au seuil de 5 % et que l'intervalle de confiance à 95 % ne contenait pas zéro.

Le test des neuf hypothèses de recherche constitue la finalité principale de la modélisation PLS-SEM. Il repose sur l'estimation des coefficients de chemin (β) du modèle structurel, qui mesurent la force et le sens des relations causales entre les construits, et sur l'évaluation de leur significativité statistique à travers les valeurs t et les p-values calculées par bootstrapping avec 5 000 ré-échantillonnages.

Pour les effets directs (H1 à H5, H8 et H9), la décision de confirmation ou d'infirmation de chaque hypothèse repose sur deux critères combinés : le sens du coefficient de chemin, qui doit être positif pour être cohérent avec la direction attendue formulée dans chaque hypothèse, et la significativité statistique, évaluée par un test de Student bilatéral au seuil de 5 % (valeur $t > 1,96$ ou p-value $< 0,05$) ou au seuil plus conservateur de 1 % (valeur $t > 2,58$ ou p-value $< 0,01$). Les intervalles de confiance au bootstrapping à 95 % constituent une information complémentaire particulièrement utile pour l'interprétation des résultats, car ils fournissent une estimation de la plage de variation probable du coefficient de chemin dans la population et permettent une décision de significativité qui ne dépend pas des hypothèses de normalité asymptotique.

Pour le test de la médiation (H6), la procédure repose sur l'analyse des effets indirects selon la méthode des intervalles de confiance au bootstrapping recommandée par Preacher et Hayes (2008), qui présente l'avantage de ne pas supposer la normalité de la distribution de l'effet indirect. La décision de médiation repose sur deux critères : la significativité de l'effet indirect (l'intervalle de confiance à 95 % ne doit pas inclure zéro) et la comparaison entre l'effet direct avant et après introduction de la variable médiatrice. Une médiation complète est conclue lorsque l'effet direct devient non significatif après introduction de la CCO dans le modèle, tandis qu'une médiation partielle est conclue lorsque l'effet direct demeure significatif mais se réduit par rapport au modèle sans médiateur. Zhao, Lynch et Chen (2010) ont enrichi ce cadre d'analyse en proposant une taxonomie des types de médiation selon la combinaison des significativités des effets direct et indirect, distinguant la médiation complémentaire, la médiation compétitive et la suppression selon la direction des effets directs et indirects.

Pour le test de la modération (H7), la procédure repose sur la construction d'un terme d'interaction entre le construit de cybersécurité (CS) et le construit de cadre réglementaire (CRI) selon la méthode des indicateurs de produit dans SmartPLS 4, et sur l'évaluation de la significativité du coefficient de chemin associé à ce terme d'interaction dans le modèle structurel. Un coefficient positif et significatif du terme d'interaction confirme que le cadre réglementaire amplifie l'effet de la cybersécurité sur la gouvernance. L'analyse des pentes simples (simple slope analysis), conduite en calculant et en comparant les effets de la cybersécurité sur la gouvernance pour des niveaux élevés, moyens et faibles du cadre réglementaire (respectivement à +1 écart-type, à la moyenne et à -1 écart-type), permet de visualiser et d'interpréter concrètement la nature de l'effet modérateur. Henseler et Fassott (2010) précisent les procédures d'implémentation de ces analyses dans SmartPLS, en soulignant l'importance de standardiser les construits avant la construction du terme d'interaction pour éviter les problèmes d'interprétation liés à la multicolinéarité entre les effets principaux et l'effet d'interaction.

4. Résultats

a. Qualité du modèle de mesure

Les indicateurs psychométriques confirment la qualité globale du modèle de mesure. Les charges externes sont satisfaisantes, avec 51 items sur 53 supérieurs à 0,70 et une charge minimale de 0,667. Les alphas de Cronbach s'inscrivent dans une plage de 0,807 à 0,890, la fiabilité composite varie

de 0,861 à 0,916, et l'AVE se situe entre 0,610 et 0,703. Le HTMT maximal observé atteint 0,499, très en deçà du seuil de 0,85, ce qui confirme la validité discriminante des construits.

Tableau 3 : Qualité explicative et prédictive du modèle structurel

Critère	Seuil	Résultat observé	Verdict
Outer loadings	> 0,70	Min. 0,667 ; 51/53 items > 0,70	Satisfaisant
Alpha de Cronbach	> 0,70	0,807 à 0,890	Excellent
Fiabilité composite ρc	> 0,80	0,861 à 0,916	Excellent
AVE	> 0,50	0,610 à 0,703	Satisfaisant
HTMT	< 0,85	Maximum 0,499	Excellent

Sur le plan de l'évaluation de la qualité de mesure, l'adoption d'un modèle de mesure réflexif implique que les indicateurs de chaque construit de premier ordre seront évalués selon les critères standard de la PLS-SEM réflexive. Henseler, Ringle et Sarstedt (2015) fournissent le cadre d'évaluation le plus complet et le plus récent pour ces critères, en distinguant la validité convergente, évaluée à travers les charges externes (outer loadings) et la variance moyenne extraite (AVE), et la validité discriminante, désormais évaluée prioritairement à travers le critère HTMT (Heterotrait-Monotrait Ratio of Correlations) dont ils ont démontré la supériorité sur les critères traditionnels de Fornell et Larcker (1981). Le respect de ces critères, qui seront vérifiés systématiquement dans le Chapitre IV, garantit que les indicateurs retenus pour chaque dimension mesurent bien le construit de premier ordre qu'ils sont censés refléter, et que les quatre dimensions de la gouvernance des PME constituent des construits empiriquement distinguables les uns des autres.

b. Qualité explicative et prédictive du modèle structurel

Les coefficients de détermination R^2 indiquent un pouvoir explicatif faible à modéré, cohérent avec la complexité des phénomènes étudiés. La transparence (TC) est la variable la mieux expliquée (R^2=0,337), suivie de la culture de cybersécurité (R^2=0,277), du contrôle interne (R^2=0,233), de la performance (R^2=0,234), de la responsabilité (R^2=0,203) et de la prise de décision stratégique (R^2=0,199). Tous les Q^2predict sont positifs, et les RMSE du modèle PLS-SEM sont inférieurs aux RMSE du modèle linéaire naïf pour l'ensemble des variables endogènes, ce qui confirme la pertinence prédictive du modèle.

Tableau 4 : Qualité explicative et prédictive du modèle structurel

Variable endogène	R^2	R^2 ajusté	Q^2predict
TC	0,337	0,303	0,246
CCO	0,277	0,262	0,241
CI	0,233	0,193	0,114
PO	0,234	0,205	0,105
RA	0,203	0,162	0,110
PD	0,199	0,158	0,069

La multicolinéarité entre les indicateurs formatifs constitue une menace statistique sérieuse pour la qualité des estimations des poids formatifs, dans la mesure où des indicateurs fortement corrélés entre eux produisent des poids instables dont l'interprétation est difficile et dont la significativité est artificiellement réduite par la variance partagée. Le variance inflation factor (VIF) constitue la mesure standard de la multicolinéarité dans ce contexte, défini comme l'inverse de la tolérance ($1 - R^2$) de la régression de chaque indicateur formatif sur les autres indicateurs du même construit. Hair et al. (2022) recommandent que les VIF soient inférieurs à 3,3 pour les construits formatifs dans la PLS-SEM, un seuil plus conservateur que le seuil usuel de 5 utilisé dans les régressions ordinaires, en raison de la sensibilité plus élevée des modèles de mesure formatifs aux effets de la multicolinéarité. Des VIF supérieurs à 3,3 indiquent une multicolinéarité problématique qui peut nécessiter la fusion ou l'élimination de certains indicateurs fortement redondants.

c. Effets directs des dimensions de cybersécurité sur la gouvernance

Anderson et al. (2013) avaient estimé que le retour sur investissement de la cybersécurité dans les PME dépend fortement du type de menace considéré : les investissements en prévention des incidents ont un retour positif seulement lorsque la probabilité et l'impact des incidents dépassent certains seuils. Dans notre modèle, la voie par laquelle la cybersécurité génère le retour sur investissement le plus robuste n'est pas directement la prévention des incidents, mais l'amélioration de la gouvernance qui en améliore la confiance partenariale, l'accès aux ressources et l'efficience opérationnelle.

Les résultats des effets directs dessinent une hiérarchie claire. Les dimensions organisationnelles et institutionnelles de la cybersécurité — politiques, formation, conformité — influencent plusieurs dimensions de gouvernance. En revanche, les technologies de protection et la gestion des incidents ne produisent pas d'effets directs significatifs sur la gouvernance dans l'échantillon étudié.

Tableau 5 : Effets directs des dimensions de cybersécurité sur la gouvernance

Relation	β	p-value	Verdict
PP → TC	0,165	0,004	Confirmée
PP → CI	0,238	<0,001	Confirmée
PP → PD	0,108	0,112	Non confirmée
PP → RA	0,117	0,061	Non confirmée au seuil de 5 %
TI → TC/CI/PD/RA	Faibles	>0,47	Non confirmée
FS → TC	0,230	<0,001	Confirmée
FS → PD	0,252	<0,001	Confirmée
FS → RA	0,189	0,003	Confirmée
FS → CI	0,109	0,072	Non confirmée au seuil de 5 %
GI → TC/CI/PD/RA	Faibles	>0,25	Non confirmée
CR → TC	0,282	<0,001	Confirmée
CR → CI	0,163	0,012	Confirmée
CR → RA	0,299	<0,001	Confirmée
CR → PD	0,060	0,400	Non confirmée

H1 est partiellement confirmée. Les politiques et procédures améliorent la transparence et le contrôle interne, car elles documentent les règles, responsabilités, accès et traces opérationnelles. En revanche, elles ne suffisent pas à transformer directement la prise de décision stratégique ni la responsabilité du dirigeant, qui exigent une appropriation plus profonde des enjeux cybernétiques.

H2 est rejetée. Les technologies et infrastructures ne produisent aucun effet direct significatif. Ce résultat ne signifie pas que la technologie est inutile ; il indique plutôt que, dans les PME marocaines, les outils techniques ne deviennent des leviers de gouvernance que lorsqu'ils sont intégrés à des politiques, compétences et routines organisationnelles. La technologie isolée reste un actif dormant.

H3 est partiellement confirmée et constitue l'un des résultats les plus robustes. La formation et la sensibilisation influencent la transparence, la prise de décision et la responsabilité. Elles transforment la cybersécurité en savoirs partagés, en réflexes comportementaux et en langage commun permettant d'intégrer le risque numérique dans les arbitrages quotidiens.

H4 est rejetée. La gestion des incidents et la continuité d'activité ne produisent pas d'effets directs significatifs. Ce résultat suggère une maturité opérationnelle encore insuffisante : l'existence déclarée de procédures ou de responsables ne suffit pas si les plans ne sont pas testés, si les sauvegardes ne sont pas régulièrement vérifiées et si les retours d'expérience ne sont pas institutionnalisés.

H5 est partiellement confirmée. La conformité réglementaire est le prédicteur le plus puissant de la transparence et de la responsabilité, et elle influence également le contrôle interne. Ce résultat confirme le rôle structurant des obligations légales et normatives dans la formalisation des pratiques de gouvernance cybernétique.

d. Médiation de la culture de cybersécurité

La culture de cybersécurité organisationnelle joue un rôle médiateur partiel et sélectif. Les politiques et procédures (β=0,247 ; p<0,001), la formation et la sensibilisation (β=0,358 ; p<0,001) et la conformité réglementaire (β=0,231 ; p<0,001) influencent significativement la culture de cybersécurité. En revanche, les technologies et la gestion des incidents ne l'influencent pas significativement. En aval, la culture de cybersécurité améliore la transparence (β=0,208 ; p=0,002), le contrôle interne (β=0,222 ; p=0,002) et la prise de décision stratégique (β=0,197 ; p=0,004), mais pas la responsabilité des dirigeants.

Tableau 6 : Médiation de la culture de cybersécurité

Relation	β	p-value	Verdict
PP → CCO	0,247	<0,001	Confirmée
FS → CCO	0,358	<0,001	Confirmée
CR → CCO	0,231	<0,001	Confirmée
TI/GI → CCO	Faibles	>0,38	Non confirmée
CCO → TC	0,208	0,002	Confirmée
CCO → CI	0,222	0,002	Confirmée
CCO → PD	0,197	0,004	Confirmée
CCO → RA	0,094	0,170	Non confirmée

Les effets indirects confirment cette médiation partielle. Les effets PP → CCO → CI, PP → CCO → PD, PP → CCO → TC, FS → CCO → CI, FS → CCO → PD, FS → CCO → TC, CR → CCO → CI, CR → CCO → PD et CR → CCO → TC sont tous significatifs. La culture de cybersécurité agit donc comme un canal de transformation : elle convertit des dispositifs formels en comportements collectifs et en pratiques de gouvernance plus robustes.

e. Modération du cadre réglementaire et institutionnel

L'hypothèse H7 n'est pas confirmée. Les vingt termes d'interaction testant l'effet modérateur du cadre réglementaire et institutionnel perçu sur les relations entre les dimensions de cybersécurité et les dimensions de gouvernance sont tous non significatifs. Les p-values sont toutes supérieures au seuil de 5 %, et les coefficients d'interaction demeurent faibles. Ce résultat montre que le cadre réglementaire, bien qu'important comme pression institutionnelle générale, ne joue pas encore un rôle différenciateur suffisant pour amplifier l'effet des pratiques cybernétiques d'une PME à l'autre.

f. Effets sur la performance organisationnelle

Les résultats relatifs à la performance confirment l'existence d'une chaîne causale cybersécurité-culture-gouvernance-performance. L'effet indirect total de la culture de cybersécurité sur la performance est significatif (β=0,112 ; t=3,372 ; p=0,001), principalement à travers la transparence et le contrôle interne. Pour H9, trois dimensions de gouvernance contribuent directement à la performance : la transparence (β=0,199 ; p=0,002), le contrôle interne (β=0,196 ; p=0,004) et la responsabilité (β=0,140 ; p=0,025). La prise de décision stratégique n'a pas d'effet direct significatif sur la performance (β=0,070 ; p=0,266).

Tableau 7 : Effets sur la performance organisationnelle

Relation	β	p-value	Verdict
CCO → PO, effet indirect total	0,112	0,001	Confirmée
TC → PO	0,199	0,002	Confirmée
CI → PO	0,196	0,004	Confirmée
RA → PO	0,140	0,025	Confirmée
PD → PO	0,070	0,266	Non confirmée

5. Discussion

a. Primauté des pratiques organisationnelles sur les solutions purement technologiques

Le résultat le plus important de cette recherche est la hiérarchie des leviers cybernétiques. Les pratiques organisationnelles — politiques formalisées, formation, sensibilisation et conformité — dominent les dimensions strictement technologiques et opérationnelles dans leur capacité à améliorer la gouvernance des PME marocaines. Cette conclusion contredit une vision technocentrée de la cybersécurité selon laquelle l'acquisition d'outils de protection constituerait la réponse principale au risque numérique.

Dans les PME à ressources limitées, la technologie n'est productive que lorsqu'elle est insérée dans un système organisationnel capable de la configurer, de l'exploiter, de l'interpréter et de la transformer en décisions. Un pare-feu, un antivirus ou une solution d'authentification ne renforcent pas la gouvernance si les responsabilités ne sont pas définies, si les alertes ne sont pas analysées,

si les collaborateurs ne comprennent pas les risques ou si les dirigeants ne reçoivent pas d'indicateurs exploitables.

Cette lecture conduit à proposer une logique de séquençage des investissements: formaliser d'abord les règles et responsabilités, sensibiliser ensuite les collaborateurs, organiser la conformité et le contrôle, puis investir dans les technologies en les reliant aux processus de gouvernance. Les outils techniques restent indispensables, mais ils ne constituent pas le point de départ le plus efficace lorsque les capacités organisationnelles sont faibles.

b. Culture de cybersécurité : un mécanisme de transmission partiel mais central

La médiation partielle de la culture de cybersécurité montre que les pratiques formelles ne produisent pas uniquement des effets par leur existence documentaire ; elles agissent également en transformant les représentations, routines et comportements des acteurs. La formation apparaît comme le déterminant le plus puissant de cette culture, ce qui confirme le rôle central du facteur humain dans les trajectoires de maturité cybernétique.

La culture ne remplace cependant pas les mécanismes formels. Elle complète les effets directs des politiques et de la conformité. Cette complémentarité est essentielle : une PME a besoin à la fois de règles explicites et de comportements intériorisés. Les règles sans culture restent bureaucratiques ; la culture sans règles reste informelle et difficilement vérifiable. La gouvernance cybernétique exige l'articulation des deux.

c. Faible effet modérateur du cadre réglementaire : un signal institutionnel

Le rejet de l'hypothèse de modération institutionnelle ne signifie pas que le cadre réglementaire marocain est sans importance. Les résultats montrent au contraire que la conformité réglementaire interne influence fortement la transparence et la responsabilité. En revanche, la perception du cadre réglementaire externe ne différencie pas suffisamment les PME pour amplifier les effets de leurs pratiques cybernétiques.

Cette situation révèle une distance entre la norme formelle et l'effet institutionnel réel. Pour qu'un cadre réglementaire joue pleinement son rôle modérateur, il doit être clairement compris, effectivement appliqué, accompagné par des outils pratiques et perçu comme contraignant par les dirigeants de PME. Dans le contexte marocain, l'existence d'un cadre légal constitue une base structurante, mais son appropriation opérationnelle par les PME demeure encore incomplète.

d. Gouvernance et performance : la cybersécurité comme investissement productif

Les résultats sur la performance confirment que la cybersécurité peut produire une valeur organisationnelle lorsqu'elle renforce la gouvernance. La transparence et le contrôle interne sont les canaux les plus robustes : une information fiable, des processus contrôlés et des responsabilités identifiables réduisent les erreurs, les interruptions, les coûts d'incident et les incertitudes relationnelles. La responsabilité des dirigeants contribue également à la performance, probablement en améliorant la discipline organisationnelle et la confiance des partenaires.

La non-significativité de la prise de décision stratégique sur la performance directe peut s'expliquer par un délai temporel. Les décisions stratégiques intégrant les risques cybernétiques produisent souvent des effets différés, qui ne sont pas toujours captés dans une enquête transversale. Elles peuvent également agir indirectement en améliorant d'abord la transparence, le contrôle ou la qualité des processus.

6. Contributions théoriques

Premièrement, l'article contribue à la théorie de l'agence en montrant que les pratiques de cybersécurité réduisent les asymétries d'information à travers la transparence et le contrôle interne. Les politiques formalisées et la conformité produisent des traces, règles et obligations qui améliorent la capacité de surveillance et de reddition de comptes.

Deuxièmement, l'article enrichit la théorie des parties prenantes en montrant que la cybersécurité n'est pas uniquement une protection interne, mais une condition de confiance vis-à-vis des clients, fournisseurs, salariés et partenaires. La formation et la responsabilité traduisent cette dimension relationnelle.

Troisièmement, il nuance la théorie institutionnelle. Le cadre légal marocain influence la gouvernance lorsqu'il est internalisé sous forme de conformité, mais ne produit pas encore d'effet modérateur externe. Ce résultat distingue l'existence formelle de la norme de son effectivité organisationnelle.

Quatrièmement, l'article contribue à la vision par les ressources en montrant que la cybersécurité devient une ressource stratégique seulement lorsqu'elle combine actifs techniques, compétences humaines, règles organisationnelles et culture partagée. Les technologies isolées ne suffisent pas à produire un avantage gouvernant ou performantiel.

7. Implications managériales et institutionnelles

a. Pour les dirigeants de PME

Les dirigeants de PME devraient éviter de réduire la cybersécurité à un budget informatique. Les résultats invitent à construire une feuille de route progressive : établir une politique simple et écrite, cartographier les actifs informationnels critiques, clarifier les responsabilités, former régulièrement les collaborateurs, documenter les incidents, tester les sauvegardes et relier les indicateurs cybernétiques aux décisions de gestion.

La priorité doit être donnée aux pratiques à fort rendement gouvernant : formalisation des règles d'accès, procédure de sauvegarde, sensibilisation au phishing, dispositif de validation des droits utilisateurs, reporting minimal des incidents et conformité aux obligations légales. Cette base permet ensuite de rentabiliser les investissements technologiques.

b. Pour les institutions d'accompagnement

Les institutions publiques, organisations professionnelles, CRI, fédérations sectorielles et programmes d'appui aux PME devraient intégrer la maturité cybernétique dans leurs dispositifs d'accompagnement. Les formations doivent être adaptées aux contraintes des PME : modules courts, guides opérationnels, modèles de politiques, check-lists de conformité, diagnostics simplifiés et outils d'auto-évaluation.

L'accompagnement devrait éviter un langage excessivement technique et relier directement la cybersécurité aux préoccupations des dirigeants : continuité d'activité, confiance client, accès au financement, relation avec les donneurs d'ordre, conformité et performance.

c. Pour les régulateurs et décideurs publics

Le rejet de l'effet modérateur du cadre réglementaire suggère la nécessité de renforcer l'effectivité perçue du dispositif institutionnel. Cela passe par une meilleure vulgarisation des obligations, des

guides adaptés aux PME, des actions sectorielles, des incitations à la mise en conformité et une articulation plus visible entre cybersécurité, protection des données et gouvernance d'entreprise.

Une approche graduée pourrait être envisagée, distinguant les obligations minimales applicables à toutes les PME, les exigences renforcées pour les PME exposées à des données sensibles, et les dispositifs d'accompagnement pour les entreprises intégrées dans des chaînes de valeur critiques.

8. Limites et perspectives de recherche

Cette recherche présente plusieurs limites. Premièrement, le design transversal ne permet pas de conclure définitivement à la causalité temporelle des relations. Une étude longitudinale permettrait de suivre l'évolution de la maturité cybernétique et ses effets différés sur la gouvernance et la performance. Deuxièmement, les données sont déclaratives et reposent sur la perception des dirigeants ; des données objectives, audits ou indicateurs techniques pourraient compléter l'analyse. Troisièmement, l'échantillon, bien que satisfaisant pour la PLS-SEM, gagnerait à être élargi et stratifié par secteur, région, taille et niveau de digitalisation.

Les recherches futures pourraient comparer les PME marocaines à celles d'autres économies émergentes, tester des modèles sectoriels, intégrer des variables telles que la maturité numérique, le soutien du top management, la pression des donneurs d'ordre ou l'intensité concurrentielle, et examiner les effets différés de la prise de décision stratégique sur la performance. Une approche mixte combinant PLS-SEM et entretiens qualitatifs permettrait également d'expliquer plus finement les mécanismes d'appropriation de la culture cybernétique.

9. Conclusion

Cet article a analysé l'impact de la cybersécurité sur la gouvernance et la performance organisationnelle des PME marocaines à travers un modèle empirique testé par PLS-SEM auprès de 246 dirigeants. Les résultats établissent que la cybersécurité constitue bien un levier de gouvernance, mais que son efficacité dépend fortement de la nature des pratiques mises en œuvre. Les politiques et procédures améliorent la transparence et le contrôle interne ; la formation influence la transparence, la décision et la responsabilité ; la conformité réglementaire constitue le prédicteur le plus puissant de la transparence et de l'accountability. En revanche, les technologies et la gestion des incidents ne produisent pas d'effets directs significatifs lorsqu'elles ne sont pas soutenues par des capacités organisationnelles complémentaires.

La culture de cybersécurité joue un rôle médiateur partiel, confirmant que la gouvernance cybernétique ne se construit pas uniquement par des règles ou des outils, mais aussi par l'intériorisation collective des comportements de sécurité. Le cadre réglementaire perçu ne joue pas encore le rôle modérateur attendu, ce qui révèle un enjeu d'effectivité institutionnelle. Enfin, la transparence, le contrôle interne et la responsabilité contribuent à la performance organisationnelle, montrant que la cybersécurité peut être pensée comme un investissement productif lorsqu'elle renforce les mécanismes de gouvernance.

La principale implication de cette recherche est claire : pour les PME marocaines, la priorité n'est pas de choisir entre technologie, conformité et formation, mais de les articuler dans une trajectoire progressive de gouvernance cybernétique. La cybersécurité devient performante lorsqu'elle cesse d'être un dispositif périphérique et devient une pratique de gouvernance intégrée.

10. Références

- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. Workshop on the Economics of Information Security.
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.
- Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. Human Relations, 61(8), 1139-1160.
- Bebchuk, L., Cohen, A., & Ferrell, A. (2009). What matters in corporate governance? Review of Financial Studies, 22(2), 783-827.
- Brown, L. D., & Caylor, M. L. (2006). Corporate governance and firm valuation. Journal of Accounting and Public Policy, 25(4), 409-434.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.
- COSO. (2013). Internal Control—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission.
- Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49, 162-176.
- Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. Computers & Security, 92, 101713.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method. Wiley.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.
- Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2006). Market value of voluntary disclosures concerning information security. MIS Quarterly, 30(3), 567-594.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2022). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. Springer.
- Henseler, J., & Fassott, G. (2010). Testing moderating effects in PLS path models: An illustration of available procedures. In V. Esposito Vinzi et al. (Eds.), Handbook of Partial Least Squares. Springer.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43, 115-135.

- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305-360.
- Monks, R. A. G., & Minow, N. (2011). Corporate governance. Wiley.
- North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press.
- Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory. McGraw-Hill.
- Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. South African Computer Journal, 31, 46-52.
- Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J. H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. European Journal of Marketing, 53(11), 2322-2347.
- Spence, M. (1973). Job market signaling. Quarterly Journal of Economics, 87(3), 355-374.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.
- Zolait, A. H. S., Ibrahim, A. R., & Farooq, S. U. (2010). A study of internet banking adoption in Yemen: An extension of the technology acceptance model. International Journal of Business and Management, 5(9), 102-112.
- Royaume du Maroc. (2020). *Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité*. Bulletin Officiel n° 6906, 6 août 2020.
- Royaume du Maroc. (2009). *Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*. Bulletin Officiel n° 5714, 5 mars 2009.