HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

محددات فاعلية إدارة أمن المعلومات في المدارس الثانوية الخاصة بالمدينة المنورة: دراسة ميدانية في ضوء مدخل التكامل المؤسسي

عثمان كمال محمود محمد أحمد[1]

[1] جامعة النيلين، السودان.

بريد الكتروني: osmankamal2000@hotmail.com

HNSJ, 2026, 7(9); https://doi.org/10.53796/hnsj79/17

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/79/17

تاريخ الاستقبال: 2026/08/08م تاريخ القبول: 2026/08/15م تاريخ النشر: 2026/09/01م

المستخلص

هدفت الدراسة إلى تحديد مستوى فاعلية إدارة أمن المعلومات في المدارس الثانوية الخاصة بالمدينة المنورة، والكشف عن الأبعاد التنظيمية والتقنية والبشرية الأكثر ارتباطًا بها وإسهامًا في تفسيرها، وتشخيص فجوة التكامل المؤسسي تمهيدًا لبناء نموذج متكامل قابل للتطبيق والقياس. اعتمدت الدراسة المنهج الوصفي التحليلي بتصميم مقطعي، واستخدمت استبانة مكونة من (51) عبارة موزعة على ثمانية محاور. وتكونت العينة من (356) مشاركًا من القيادات المدرسية والمعلمين والإداريين والعاملين في تقنية المعلومات والإشراف التقني. وأظهرت الأداة مستوى مرتفعًا من الاتساق الداخلي؛ إذ بلغ معامل ألفا كرونباخ للدرجة الكلية (0.979)، وتراوحت معاملات المحاور بين (0.859–0.955). وأظهرت النتائج أن جميع محاور الدراسة جاءت بمستوى مرتفع أو مرتفع جدًا؛ إذ تصدرت الحاجة إلى نموذج متكامل بمتوسط (4.496)، تلتها فاعلية إدارة أمن المعلومات (4.269)، ثم الضوابط التقنية (4.265)، في حين جاءت السياسات والإجراءات في المرتبة الأخيرة نسبيًا بمتوسط (4.039). كما ارتبطت الفاعلية ارتباطًا موجبًا ودالًا إحصائيًا بالسياسات والإجراءات(r=0.679) ، والوعي الأمني (r=0.653)، والحوكمة .(r=0.623) وفسّر نموذج الانحدار المتعدد (57.1%) من التباين في الفاعلية، وكانت السياسات والإجراءات(β=0.396) ، والحوكمة(β=0.301) ، والوعي الأمني (β=0.288) أبرز المتنبئات الإيجابية. كذلك ظهرت فروق دالة في الفاعلية العامة لصالح الحاصلين على تدريب في الأمن السيبراني. وخلصت الدراسة إلى أن التحدي الرئيس لا يتمثل في غياب الضوابط الأساسية، بل في ضعف تكاملها واستدامتها ضمن دورة مؤسسية موحدة. وأوصت بتطبيق نموذج متدرج يربط الحوكمة والسياسات والمخاطر والضوابط والحوادث والتدريب ومؤشرات الأداء، مع التحقق ميدانيًا من فاعلية نظام *EduSec* الداعم.

الكلمات المفتاحية: أمن المعلومات، الأمن السيبراني، الحوكمة، إدارة المخاطر، التكامل المؤسسي، المدارس الخاصة، *EduSec*.

RESEARCH TITLE

Determinants of Information Security Management Effectiveness in Private Secondary Schools in Madinah: A Field Study in Light of the Institutional Integration Approach

Abstract

This study aimed to determine the level of information security management effectiveness in private secondary schools in Madinah, identify the organizational, technical, and human dimensions most strongly associated with and contributing to its effectiveness, and diagnose the institutional integration gap as a foundation for developing an integrated, applicable, and measurable model. The study employed a cross-sectional descriptive-analytical design and used a 51-item questionnaire covering eight dimensions. The sample comprised 356 participants, including school leaders, teachers, administrators, information technology personnel, and technical supervisors. The instrument demonstrated high internal consistency, with an overall Cronbach's alpha of 0.979 and coefficients for the individual dimensions ranging from 0.859 to 0.955. The findings indicated that all dimensions were rated high or very high. The need for an integrated model ranked first (M = 4.496), followed by information security management effectiveness (M = 4.269) and technical controls (M = 4.265), whereas policies and procedures ranked relatively last (M = 4.039). Effectiveness was positively and significantly correlated with policies and procedures (r = 0.679), security awareness (r = 0.653), and governance (r = 0.623). The multiple regression model explained 57.1% of the variance in effectiveness, with policies and procedures (β = 0.396), governance (β = 0.301), and security awareness (β = 0.288) emerging as the strongest positive predictors. Significant differences in overall effectiveness were also found in favor of participants who had received cybersecurity training. The study concluded that the primary challenge lies not in the absence of basic controls but in their insufficient integration and sustainability within a unified institutional cycle. It recommended implementing a phased model that integrates governance, policies, risks, controls, incidents, training, and performance indicators, while empirically evaluating the effectiveness of the supporting *EduSec* system.

Key Words: Information security; cybersecurity; governance; risk management; institutional integration; private schools; EduSec.

المقدمة

أصبحت المؤسسات التعليمية بيئات رقمية كثيفة الاعتماد على نظم معلومات الطلاب، ومنصات التعلم، والحوسبة السحابية، والبريد المؤسسي، وأجهزة المستخدمين، وهو ما وسّع نطاق الأصول والبيانات والتهديدات وفي المدرسة الخاصة تتقاطع متطلبات الاستمرارية التعليمية وحماية بيانات الطلاب والعاملين مع محدودية الموارد وتعدد مزودي الخدمات، الأمر الذي يجعل إدارة أمن المعلومات قضية حوكمة مؤسسية وليست مهمة تقنية منفردة.

تؤكد أطر الإدارة الحديثة أن الأمن الفاعل يقوم على دورة مترابطة تبدأ بالحوكمة وتقييم المخاطر، ثم اختيار الضوابط وتشغيلها، والكشف عن الحوادث والاستجابة لها والتعلم منها، مع بناء ثقافة أمنية قابلة للقياس .ومع ذلك، اتجهت نسبة معتبرة من الدراسات التعليمية العربية إلى قياس الوعي أو دور القيادة أو توافر بعض الممارسات كلٌّ على حدة، بينما ظل التكامل بين السياسة والمخاطر والضوابط والحوادث والوعي أقل تناولًا، ولا سيما في المدارس الثانوية الخاصة بالمدينة المنورة.

مشكلة الدراسة

تتمثل المشكلة في احتمال وجود مفارقة بين ارتفاع توافر الضوابط الأساسية وبين ضعف تكاملها واستدامتها داخل نظام إداري موحد. فوجود النسخ الاحتياطي أو الحماية من البرمجيات الضارة لا يضمن وحده وضوح المسؤوليات، أو انتظام مراجعة المخاطر، أو نشر السياسات، أو تحليل أسباب الحوادث. وعليه تسأل الدراسة:

ما مستوى فاعلية إدارة أمن المعلومات في المدارس الثانوية الخاصة بالمدينة المنورة، وما الأبعاد الأكثر ارتباطًا بها وتفسيرًا لها، وما دلالة ذلك لبناء نموذج تكاملي قابل للتشغيل والقياس؟

أهداف الدراسة

- قياس مستوى الحوكمة والسياسات وإدارة المخاطر والضوابط التقنية وإدارة الحوادث والوعي الأمني وفاعلية الإدارة
- اختبار العلاقات بين أبعاد إدارة أمن المعلومات والفاعلية المدركة
- تحديد الأبعاد الأكثر إسهامًا في تفسير فاعلية إدارة أمن المعلومات
- تشخيص الفجوات ذات الأولوية واقتراح مسار مؤسسي متكامل للتحسين
- **فرضيات الدراسة**
- توجد علاقات ارتباطية موجبة دالة إحصائيًا بين أبعاد إدارة أمن المعلومات وفاعليتها.
- تسهم الحوكمة والسياسات وإدارة المخاطر والضوابط التقنية وإدارة الحوادث والوعي الأمني إسهامًا دالًا في تفسير فاعلية إدارة أمن المعلومات
- توجد فروق في بعض تقديرات الفاعلية تبعًا للخصائص الوظيفية والتنظيمية والتدريبية لأفراد العينة

الإطار النظري والدراسات السابقة

يعبر أمن المعلومات عن حماية سرية المعلومات وسلامتها وتوافرها، مع امتداد الإدارة الحديثة إلى المساءلة والمرونة والامتثال والخصوصية ويضع معيار *ISO/IEC 27001* إدارة المخاطر والتحسين المستمر في قلب نظام إدارة أمن المعلومات، بينما يجمع إطار *NIST* للأمن السيبراني بين الحوكمة والتحديد والحماية والكشف والاستجابة والتعافي

ويضيف *COBIT* منظور المواءمة بين الحوكمة والإدارة وقيمة المؤسسة وتلتقي هذه الأطر عند رفض اختزال الأمن في شراء أدوات منفصلة.

بينت *Da Veiga et al (2020)* أن ثقافة أمن المعلومات بنية تنظيمية تتشكل من القيم والسياسات والممارسات والسلوك، وقدم *Ocloo et al. (2021)* إطارًا لمؤسسات التعليم العالي يربط الأشخاص والسياسات والتشغيل والتقنية، كما أظهرت دراسة *Nævestad et al (2023)* أن الجهود النظامية لتحسين نظام الإدارة والثقافة الأمنية ترتبط بتحسن السلوك، وأشارت *Lamond et al (2025)* إلى أن التعليم السيبراني المدرسي قد يظل متقطعًا عند غياب الموارد والدعم المؤسسي .

عربيًا وجدت المنتشري وحريري (2020) أن التدريب عامل فارق في الوعي، وأبرزت المنتشري (2020) مركزية القيادة المدرسية، في حين تناولت السمحان (2020) المتطلبات المؤسسية للأمن السيبراني في نظم المعلومات الإدارية. وتعد دراسة الظويفري (2021) الأقرب مكانيًا؛ إذ وجدت ارتفاع واقع الأمن السيبراني في مدارس التعليم العام بالمدينة المنورة مع استمرار تحديات تطبيقية غير أن الأدبيات السابقة لم تجمع في سياق المدارس الثانوية الخاصة، بين ثمانية أبعاد واختبار علاقاتها التنبؤية ثم ترجمتها إلى متطلبات تشغيلية؛ وهي الفجوة التي تعالجها الدراسة الحالية.

المنهجية

التصميم والمجتمع والعينة

اتبعت الدراسة المنهج الوصفي التحليلي بتصميم مقطعي، استهدف المجتمع العاملين في المدارس الثانوية الخاصة بالمدينة المنورة من القيادات والمعلمين والإداريين والعاملين في تقنية المعلومات والإشراف التقني. ووزعت الاستبانة إلكترونيًا، وبلغ عدد الاستجابات المكتملة الصالحة للتحليل (356). ونظرًا إلى عدم توافر إطار معاينة مكتمل في البيانات النهائية المتاحة، تعاملت الدراسة مع العينة بوصفها عينة استجابية غير احتمالية؛ ولذلك تفسر النتائج في حدود المشاركين ولا تُعمم احتماليًا على جميع المدارس دون تحفظ .

يبين الجدول التالي خصائص المشاركين. غلبت فئة المعلمين (73.6%)، وبلغت نسبة ذوي الخبرة عشر سنوات فأكثر (55.1%)، في حين أفاد **(30.3%)** فقط بحضور تدريب في الأمن السيبراني.

المتغير	الفئة	ن	%
المسمى الوظيفي	مدير/وكيل	36	10.1
	معلم/ة	262	73.6
	إداري/ة	25	7
	تقنية معلومات/إشراف تقني	33	9.3
الخبرة	أقل من 5 سنوات	68	19.1
	5إلى أقل من 10	92	25.8
	10سنوات فأكثر	196	55.1
التدريب السيبراني	نعم	108	30.3
	لا	248	69.7

المصدر :إعداد الباحث من بيانات الدراسة الميدانية

أداة الدراسة وصدقها وثباتها

تكونت الأداة من (51) عبارة موزعة على ثمانية محاور: الحوكمة (6)، السياسات والإجراءات (6)، إدارة المخاطر (6)، الضوابط التقنية(8) ، إدارة الحوادث (6)، الوعي الأمني (8)، فاعلية إدارة أمن المعلومات (7)، والحاجة إلى النموذج المقترح (4) استخدم مقياس ليكرت الخماسي من (1) لا أوافق بشدة إلى (5) أوافق بشدة. تحقق الاتساق الداخلي من خلال ارتباط العبارة بمحورها، وكانت الارتباطات دالة عند مستوى (0.01)، وبلغ ألفا كرونباخ للدرجة الكلية (0.979)، وتراوحت معاملات المحاور بين (0.859–0.955)، بما يدعم اتساق الأداة الداخلي .

التحليل الإحصائي

استخدمت التكرارات والنسب، والمتوسطات والانحرافات المعيارية، ومعامل ارتباط بيرسون، والانحدار الخطي المتعدد بطريقة الإدخال المتزامن، واختبار ت للعينات المستقلة، وتحليل التباين الأحادي واختبار شيفيه عند الحاجة.

فُسر المتوسط وفق الفئات:

- منخفض جدًا منخفض جدًا (1.00–أقل من 1.80).
- منخفض (1.80–أقل من 2.60).
- متوسط (2.60–أقل من 3.40).
- مرتفع (3.40–أقل من 4.20).
- ومرتفع جدًا (4.20–5.00).

مع اعتماد مستوى دلالة إحصائية ($\alpha = 0.05$).

الاعتبارات الأخلاقية

اقتصر جمع البيانات على أغراض البحث، وكانت المشاركة طوعية، وعولجت الاستجابات بصورة مجمعة دون إظهار هوية الأفراد أو المدارس، ولم تتضمن الأداة طلب كلمات مرور أو بيانات تشغيلية حساسة أو سجلات حوادث قابلة لإسنادها إلى مدرسة بعينها .

النتائج

النتائج الوصفية

جاءت جميع المحاور بمستوى مرتفع أو مرتفع جدًا، تصدرت الحاجة إلى النموذج المتكامل بمتوسط (4.496)، وهو أعلى من متوسطات الممارسات القائمة، بما يكشف اتفاق المشاركين على وجود حاجة إلى إطار جامع رغم التقدير الإيجابي للواقع، وجاءت السياسات والإجراءات (4.039) وإدارة المخاطر (4.058) والوعي(4.096) في أدنى المراتب النسبية .

الترتيب	المحور	المتوسط	الانحراف	التحقق %	المستوى
1	الحاجة إلى النموذج المقترح	4.496	0.523	89.9	مرتفع جدًا
2	فاعلية إدارة أمن المعلومات	4.269	0.481	85.4	مرتفع جدًا
3	الضوابط التقنية	4.265	0.586	85.3	مرتفع جدًا
4	حوكمة أمن المعلومات	4.189	0.534	83.8	مرتفع
5	إدارة الحوادث الأمنية	4.168	0.652	83.4	مرتفع
6	الوعي الأمني	4.096	0.569	81.9	مرتفع
7	إدارة المخاطر الأمنية	4.058	0.711	81.2	مرتفع
8	السياسات والإجراءات	4.039	0.616	80.8	مرتفع

المصدر :إعداد الباحث من نتائج التحليل الإحصائي (ن=356)

على مستوى العبارات، ظهر نمط متكرر: كانت الضوابط الأساسية الأعلى، مثل النسخ الاحتياطي (4.438) والحماية من الفيروسات (4.343)، في حين انخفضت نسبيًا الممارسات التي تتطلب انتظامًا مؤسسيًا، مثل إطلاع العاملين على الإجراءات(3.840) ، والتدريب الدوري (3.963)، وخطط معالجة المخاطر (4.017)، ورصد الأنشطة غير المعتادة (4.067)، وتحليل أسباب الحوادث(4.112) .

العلاقات الارتباطية

كانت جميع العلاقات بين المحاور موجبة ودالة عند ($p<0.01$) ارتبطت الفاعلية بصورة أقوى بالسياسات والإجراءات ($r=0.679$)، ثم الوعي الأمني($r=0.653$) ، والحوكمة($r=0.623$) ، وإدارة الحوادث($r=0.58$) ، والضوابط التقنية ($r=0.523$)، وإدارة المخاطر .($r=0.502$) كما ارتفعت الارتباطات البينية بين المخاطر والحوادث ($r=0.874$) وبين الضوابط والحوادث($r=0.839$) ، بما يدل على ترابط تشغيلي قوي بين هذه الوظائف .

نموذج الانحدار المتعدد

كان نموذج الانحدار دالًّا إحصائيًّا؛ إذ بلغت قيمة اختبار ف($F = 77.40$) ، عند مستوى دلالة ($p < 0.001$) وقد فسَّرت المتغيرات الستة مجتمعةً ما نسبته (57.1%) من التباين في فاعلية إدارة أمن المعلومات، حيث بلغ معامل التحديد ($R^2 = 0.571$)وأظهرت النتائج أن بُعد السياسات والإجراءات كان أقوى المتنبئات الإيجابية بفاعلية إدارة أمن المعلومات، تلاه كلٌّ من الحوكمة، والوعي الأمني، وإدارة الحوادث.

المتغير	β	اتجاه الأثر	الاستنتاج
السياسات والإجراءات	0.396	موجب	أقوى متنبئ بالفاعلية
الحوكمة	0.301	موجب	أثر قيادي وتنظيمي واضح
الوعي الأمني	0.288	موجب	الثقافة والسلوك عنصران حاسمان
إدارة الحوادث	0.248	موجب	تعزز الاستجابة والتعلم المؤسسي
إدارة المخاطر	−0.238	انعكاس جزئي	يفسر بحساسية التداخل الخطي
الضوابط التقنية	−0.19	انعكاس جزئي	لا يفسر كعلاقة سببية عكسية

ملاحظة :ظهرت إشارتا المخاطر والضوابط سالبتين بعد ضبط بقية المتغيرات رغم ارتباطهما البسيط الموجب بالفاعلية؛ وبلغ *VIF* نحو 5.13 للمخاطر، و4.41 للضوابط، و6.82 للحوادث، لذا تُفسر الإشارتان في سياق التداخل الخطي ولا تُعاملان كأثرين سببيين عكسيين.

الفروق بين المشاركين

لم تظهر فروق ذات دلالة إحصائية بين الحاصلين على التدريب وغير الحاصلين عليه في معظم محاور الدراسة، في حين ظهر فرق دال إحصائيًا في مستوى الفاعلية العامة لصالح الحاصلين على التدريب؛ إذ بلغ المتوسط الحسابي لديهم (4.360)، مقابل (4.230) لغير الحاصلين عليه، وبلغت قيمة اختبار ت($t = 2.358$) ، عند مستوى دلالة ($p = 0.019$)كما كشفت المقارنات وفقًا لمتغيرات الوظيفة، وسنوات الخبرة، وحجم المدرسة عن وجود فروق دالة إحصائيًا في بعض المحاور، مما يشير إلى تباين إدراك أفراد العينة داخل المؤسسات التعليمية. ومع ذلك، ينبغي تفسير النتائج المرتبطة بهذه المتغيرات بحذر؛ نظرًا إلى صغر حجم بعض الفئات الوظيفية، ولا سيما فئتي موظفي تقنية المعلومات ومديري المدارس.

المناقشة

تكشف النتائج أن المدارس محل الدراسة تمتلك قاعدة جيدة من الضوابط والممارسات، لكنها لم تبلغ بالضرورة مستوى النضج المؤسسي المتكامل ويؤيد ذلك تصدر الحاجة إلى النموذج المقترح، مع وقوع السياسات والمخاطر والوعي في المراتب النسبية الأدنى فالاختلاف بين توافر النسخ الاحتياطي والحماية من الفيروسات من جهة، وبين انخفاض نشر الإجراءات والتدريب الدوري ومعالجة المخاطر والرصد الاستباقي من جهة أخرى، يعكس انتقال موضع الفجوة من اقتناء الضابط إلى تشغيله واستدامته ومراجعته .

تتفق النتيجة العامة مع الظويفري (2021) في ارتفاع واقع الأمن السيبراني بمدارس المدينة المنورة مع استمرار تحديات تطبيقية، وتنسجم مع *Da Veiga et al (2020)* و *Ocloo et al (2021)* في أن الثقافة والسياسات والعمليات والتقنية مكونات مترابطة. كما تدعم دراسة *Nævestad et al (2023)* تفسير أن التحسن المستدام يرتبط بالجهود النظامية لا بالإجراءات المنعزلة ويختلف المستوى المرتفع للوعي في الدراسة الحالية عن نتائج بعض الدراسات العربية الأقدم التي رصدت وعيًا ضعيفًا أو متوسطًا؛ وقد يرجع ذلك إلى التطور الرقمي والتنظيمي، وإلى أن الدراسة الحالية تقيس ممارسات مؤسسية من فئات وظيفية متعددة لا معرفة فردية فقط .

تقدم نتائج الانحدار دليلًا إضافيًا وهو أن تفوق السياسات والحوكمة والوعي على الضوابط التقنية في تفسير الفاعلية يعني أن التقنية تحقق قيمتها حين تُوجَّه بسياسة واضحة ومسؤوليات محددة ومتابعة وتدريب. أما ارتفاع الترابط بين المخاطر والضوابط والحوادث فيدعم تصميم سير عمل موحد يربط الأصل والخطر والضابط والحادثة والإجراء التصحيحي بدل إدارة سجلات متفرقة .

أما أثر التدريب المحدود في معظم المحاور، فلا ينفي أهميته؛ إذ إن متغير الحضور الثنائي لا يقيس جودة التدريب أو حداثته أو جرعته أو أثره السلوكي وتتمثل الدلالة العملية في ضرورة الانتقال من دورات عامة إلى برنامج قائم على المخاطر والأدوار، مع قياس قبلي وبعدي ومحاكاة تصيد ومؤشرات التزام .

الدلالات التطبيقية والنموذج المقترح

تقترح الدراسة مسارًا تكامليًا يبدأ بتكليف حوكمي واضح، ثم حصر الأصول وتصنيف البيانات وتقييم المخاطر، وربط المخاطر بضوابط ومسؤولين ومواعيد، وتشغيل قنوات موحدة للإبلاغ والاستجابة، ثم تحليل السبب الجذري والتعلم، وربط ذلك بالتدريب ومؤشرات النضج ويمكن لنظام *EduSec* دعم هذا المسار عبر سجلات مترابطة ولوحات قياس وتنبيهات وأدلة امتثال. غير أن النظام في وضعه الحالي نموذج أولي ومحاكاة تشغيلية، ولا تعد مؤشرات تشغيله دليلًا سببيًا نهائيًا قبل اختباره ميدانيًا .

- اعتماد لجنة ومسؤوليات واضحة لأمن المعلومات وربطها بالقيادة المدرسية.
- تحويل السياسات إلى دورة حياة تشمل النشر والإقرار والمراجعة وإدارة الاستثناءات.
- إنشاء سجل أصول ومخاطر وربط كل خطر بخطة معالجة ومالك وموعد ومؤشر.
- تعزيز الرصد الاستباقي والمصادقة متعددة العوامل ومراجعة الصلاحيات.
- توحيد الإبلاغ عن الحوادث والتصعيد وتحليل الأسباب والدروس المستفادة.
- تنفيذ تدريب دوري قائم على الدور والمخاطر وقياس الأثر السلوكي.
- تجريب *EduSec* تدريجيًا وقياس النضج وزمن الاستجابة وجودة السجلات قبل التوسع.

حدود الدراسة واتجاهات البحث المستقبلي

تحد النتائج طبيعة التصميم المقطعي والاعتماد على التقرير الذاتي، وعدم توافر إطار معاينة يسمح بتعميم احتمالي، وعدم توازن الفئات الوظيفية، واحتمال تحيز الرغبة الاجتماعية. كما أن ارتفاع الارتباطات بين بعض المتغيرات يقتضي التحقق اللاحق من التمييز البنائي بينها باستخدام التحليل العاملي التوكيدي أو نمذجة المعادلات الهيكلية. وتقترح الدراسة تنفيذ تجربة قبلية وبعدية لنظام *EduSec* ، وتطوير مقياس نضج خاص بالمؤسسات التعليمية، وإجراء مقارنات بين المدارس الحكومية والخاصة والمناطق المختلفة، واستخدام مؤشرات سلوكية وتشغيلية فعلية إلى جانب الاستبانة.

الخاتمة

خلصت الدراسة إلى أن فاعلية إدارة أمن المعلومات في المدارس الثانوية الخاصة بالمدينة المنورة مرتفعة من منظور المشاركين، غير أن القوة النسبية للضوابط الأساسية تتعايش مع فجوات في نشر السياسات والتدريب ومعالجة المخاطر والرصد والتعلم من الحوادث وكانت السياسات والحوكمة والوعي أهم محددات الفاعلية، بينما أكد تصدر الحاجة إلى نموذج متكامل أن الارتفاع الوصفي لا يساوي النضج. وعليه، فإن التحسين الأكثر جدوى هو بناء دورة مؤسسية موحدة قابلة للقياس، لا إضافة أدوات تقنية منفصلة.

الإقرارات

- **تعارض المصالح:** يصرح الباحث بعدم وجود تعارض مصالح.
- **التمويل:** لم تتلق الدراسة تمويلًا مخصصًا من جهة تمويل عامة أو تجارية أو غير ربحية.
- **إتاحة البيانات:** تتضمن البيانات استجابات مؤسسية حساسة نسبيًا، ويمكن النظر في إتاحة نسخة منزوعة الهوية وفق الضوابط الأخلاقية وموافقة الجهة المختصة.
- **إسهام المؤلف:** تولى الباحث تصميم الدراسة وجمع البيانات وتحليلها وكتابة الورقة.

المراجع

المراجع العربية

1. الصحفي، مصباح أحمد حامد، وعسكول، سناء صالح. (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية، 20*(10)، 493-534. https://doi.org/10.21608/jsre.2019.56490

Al-Sahafi, M. A. H., & Askol, S. S. (2019). The level of cybersecurity awareness among female computer teachers at the secondary-school level in Jeddah. *Journal of Scientific Research in Education, 20*(10), 493–534. [In Arabic].

https://doi.org/10.21608/jsre.2019.56490

2. السمحان، منى عبد الله صالح. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. *مجلة كلية التربية بالمنصورة، 111*(1)، 2-29. https://doi.org/10.21608/maed.2010.140786

Al-Samhan, M. A. S. (2020). Requirements for achieving cybersecurity for management information systems at King Saud University. *Journal of the Faculty of Education, Mansoura University, 111*(1), 2–29. [In Arabic]. https://doi.org/10.21608/maed.2010.140786

3. المطيري، مشاعل شبيب مطيران الظويفري. (2021). واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية، 10*(3)، 635-655. https://doi.org/10.31559/EPS2021.10.3.7.655

Al-Mutairi, M. S. M. Al-Dhuwairi. (2021). The status of cybersecurity and ways of enhancing its effectiveness in public education schools in the Madinah region from the perspective of school leadership. *International Journal of Educational and Psychological Studies, 10*(3), 635–655. [In Arabic]. https://doi.org/10.31559/EPS2021.10.3.7

4. المنتشري، فاطمة يوسف. (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية، 4*(17)، 457-484. https://doi.org/10.33850/jasep.2020.100703

Al-Muntashiri, F. Y. (2020). The role of school leadership in promoting cybersecurity in public girls' schools in Jeddah from female teachers' perspectives. *Arab Journal of Educational and Psychological Sciences, 4*(17), 457–484. [In Arabic]. https://doi.org/10.33850/jasep.2020.100703

5. المنتشري، فاطمة يوسف، وحريري، رندة أحمد. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية، 4*(14)، 95=140. https://doi.org/10.33850/ejev.2020.101830

Al-Muntashiri, F. Y., & Hariri, R. A. (2020). The degree of cybersecurity awareness among female middle-school teachers in public schools in Jeddah from the teachers' perspectives. *Arab Journal of Specific Education, 4*(14), 95–140. [In Arabic]. https://doi.org/10.33850/ejev.2020.101830

المراجع الأجنبية

1) *Da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. Computers & Security, 92, 101713.*

2) *International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.*

3) *Lamond, M., Prior, S., Renaud, K., & Wood, L. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. Discover Education.*

4) *Nævestad, T.-O., Honerud, J. H., & Meyer, S. F. (2023). Information security behaviour in an organisation providing critical infrastructure: A pre-post study of efforts to improve information security culture. Springer.*

5) *National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce.*

6) *Ocloo, C., da Veiga, A., & Kroeze, J. (2021). A conceptual information security culture framework for higher learning institutions. Human Aspects of Information Security and Assurance (HAISA).*