

Final Project 2

PMG 497

نموذج المشروع النهائي ٢

أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات

أسم الطالب

معاذ التركي

المشروع النهائي- ٢

كلية الإدارة- جامعة ميدأوشن

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

الشكر والتقدير

الإهداء

مستخلص الدراسة

الهدف:

المنهجية:

النتائج:

التطبيقات والأهمية:

الكلمات المفتاحية:

جدول المحتويات

٢	الشكر والتقدير.....
٣	الإهداء.....
٤	مستخلص الدراسة.....
٧	١. الفصل الأول: الإطار العام للدراسة.....
٨	١,١. المقدمة:.....
٩	١,٢. مشكلة الدراسة.....
٩	١,٢,١. فجوات على المستوى النظري.....
٩	١,٢,٢. فجوات على المستوى التطبيقي.....
٩	١,٣. أهمية الدراسة.....
٩	١,٣,١. على المستوى النظري:.....
٩	١,٣,٢. على المستوى التطبيقي:.....
١٠	١,٤. أسئلة الدراسة.....
١٠	١,٥. أهداف الدراسة.....
١٠	١,٦. فرضيات الدراسة.....
١٠	١,٧. نموذج الدراسة.....
١١	١,٨. الدراسة الميدانية.....
١١	١,٩. مخطط المشروع.....
١٢	٢. الفصل الثاني: الدراسات السابقة.....
١٣	٢,١. المقدمة:.....
١٣	٢,٢. المتغير المستقل.....
١٣	٢,٣. المتغير التابع.....
١٤	٢,٤. العلاقة بين المتغير المستقل والمتغير التابع.....
١٤	٢,٥. الخاتمة.....
١٥	٣. الفصل الثالث: منهجية الدراسة.....

١٦	٣,١.المقدمة
٣,٢	التعريفات الإجرائية لمتغيرات البحث
٣,٣	تصميم البحث
٣,٤	مجتمع البحث وطرق وتقنيات أخذ العينات
٣,٥	طريقة جمع البيانات
٣,٦	أنواع البيانات
٣,٧	إجراءات التحليل الإحصائي
٥٧	٣,٨.الخاتمة
٥٨	٤. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج
٥٩	4.1.المقدمة
٥٩	4.2.توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)
٥٩	4.3.اختبارات الصدق والثبات للاستبيانات
٦٠	4.4.الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)
٦٠	4.5.اختبار الفرضيات ومناقشة النتائج
٦٠	٤,٦.الخاتمة
٦١	٥. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات
٦٢	٥,١.حدود الدراسة والدراسات المستقبلية:
٦٢	٥,٢.توصيات الدراسة:
٦٢	٥,٣.الخاتمة:
٦٣	قائمة المراجع
٦٤	الملاحق

جدول الأشكال

جدول الجداول

١. الفصل الأول: الإطار العام للدراسة

١,١ . المقدمة:

تشمل المقدمة الخمس مراحل لكتابة المقدمة

تكتب المقدمة في صورة فقرات فقط

١,٢. مشكلة الدراسة

يتم كتابة مقدمة بسيطة في شكل فقرة

يتم تقسيم المشكلة الى فجوات نظرية وعملية

١,٢,١. فجوات على المستوى النظري

١,٢,٢. فجوات على المستوى التطبيقي

ينتهي هذا الجزء بالسؤال الرئيسي

١,٣. أهمية الدراسة

١,٣,١. على المستوى النظري:

١,٣,٢. على المستوى التطبيقي:

١,٤ . أسئلة الدراسة

١,٥ . أهداف الدراسة

١,٦ . فرضيات الدراسة

١,٧ . نموذج الدراسة

١,٨ . الدراسة الميدانية

١,٩ . مخطط المشروع

٢. الفصل الثاني: الدراسات السابقة

٢,١. المقدمة:

٢,٢. المتغير المستقل

٢,٣. المتغير التابع

٢,٤ . العلاقة بين المتغير المستقل والمتغير التابع

٢,٥ . الخاتمة

٣. الفصل الثالث: منهجية الدراسة

تُعَدّ منهجية الدراسة الإطار العلمي المنظم الذي يُترجم الإشكالية البحثية وأهدافها إلى خطوات إجرائية قابلة للتطبيق والقياس، إذ تُحدّد الطريقة التي يسلكها الباحث للوصول إلى نتائج موثوقة قادرة على الإجابة عن أسئلة الدراسة واختبار فرضياتها. ومن هذا المنطلق، يستعرض هذا الفصل الإجراءات المنهجية التي اتّبعتها الباحثة لدراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

ويتناول الفصل بشكل متسلسل: التعريفات الإجرائية لمتغيرات البحث، وتصميم البحث ممثلاً بالبوصلية البحثية، ثم مجتمع الدراسة والعينة وأسلوب اختيارها بالأرقام الفعلية، يليه عرض لأساليب وأدوات جمع البيانات، ثم تصنيف أنواع البيانات المستخدمة، وأخيراً الإجراءات الإحصائية التي اعتمدها الباحث لتحليل البيانات واختبار الفرضيات. وقد روعي في بناء هذه المنهجية الاتساق التام بين أهداف الدراسة وفرضياتها وأدوات قياسها، بما يضمن الصدق العلمي للنتائج وقابليتها للتعميم ضمن حدود الدراسة.

3.2. التعريفات الإجرائية لمتغيرات البحث

تتبنّى الدراسة تعريفات إجرائية محددة للمتغيرات بما يجعلها قابلة للقياس الميداني عبر أداة الاستبانة، وفيما يلي بيان ذلك:

أولاً: المتغير المستقل - تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) يُقصد به إجرائياً درجة التزام الوزارات الحكومية في المنطقة الشرقية بتطبيق الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة عن الهيئة، كما يُدركها العاملون في إدارات تقنية المعلومات والأمن السيبراني، ويُقاس من خلال خمسة أبعاد فرعية على النحو الآتي:

البُعد الأول - حوكمة الأمن السيبراني: ويُقصد به إجرائياً مدى توافر السياسات والاستراتيجيات والأدوار والمسؤوليات المعتمدة لإدارة الأمن السيبراني داخل الوزارة، ويُقاس بأربع فقرات.

البُعد الثاني - تعزيز الأمن السيبراني: ويُقصد به إجرائياً مدى تطبيق الضوابط التقنية لحماية الأصول المعلوماتية مثل إدارة الهويات والوصول، وحماية الأنظمة والشبكات، وإدارة الثغرات، ويُقاس بأربع فقرات.

البُعد الثالث – صمود الأمن السيبراني: ويُقصد به إجراءات مدى جاهزية الوزارة لاستمرارية أعمالها أثناء الحوادث السيبرانية، بما يشمل خطط الاستجابة والتعافي والنسخ الاحتياطي، ويُقاس بأربع فقرات.

البُعد الرابع – الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية: ويُقصد به إجراءات مدى ضبط الوزارة للمخاطر السيبرانية الناشئة عن المتعاقدين ومزودي الخدمات السحابية، ويُقاس بأربع فقرات.

البُعد الخامس – الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية: ويُقصد به إجراءات مدى تطبيق الضوابط المتعلقة بأنظمة التشغيل والتحكم في البيانات الحكومية التي تتضمن مكونات تشغيلية، ويُقاس بأربع فقرات.

ثانياً: المتغير التابع – الجاهزية للتصدي للاختراقات: يُقصد به إجراءات قدرة الوزارة على الوقاية من الهجمات السيبرانية، واكتشافها في وقت مبكر، والاستجابة لها، والتعافي منها بفاعلية، ويُقاس بوصفه متغيراً أحادي المحور باثنتي عشرة فقرة تغطي مجتمعة هذه القدرات الأربع.

3.3. تصميم البحث (البوصلة البحثية)

اعتمدت الدراسة المنهج الوصفي التحليلي بأسلوبه الكمي بوصفه الأنسب لطبيعة الإشكالية البحثية وأهدافها، إذ يهدف إلى وصف ظاهرة تطبيق معايير NCA وقياس أثرها الإحصائي على جاهزية الوزارات. ويوضح الجدول الآتي البوصلة البحثية التي تمثل الإطار المرجعي للقرارات المنهجية:

العنصر المنهجي	الاختيار في الدراسة	المبرر
الفلسفة البحثية	الوضعية (Positivism)	ملاءمتها لاختبار الفرضيات وقياس العلاقات السببية بأدوات موضوعية
المدخل البحثي	الاستنباطي (Deductive)	الانطلاق من إطار نظري قائم (ضوابط NCA) نحو اختبار فرضيات ميدانية
المنهج	الوصفي التحليلي – الكمي	يجمع بين وصف الواقع وتحليل العلاقات بين المتغيرات
الاستراتيجية	المسح الميداني (Survey)	فاعليته في الوصول إلى عينة واسعة في وقت محدود

الأفق الزمني	مقطعي (Cross-Sectional)	جمع البيانات في فترة زمنية واحدة محددة
أداة جمع البيانات	الاستبانة الإلكترونية	الموضوعية والقدرة على الوصول الجغرافي الواسع
أسلوب التحليل	كمي - إحصائي باستخدام SPSS	ملاءمته لاختبار فرضيات تتعلق بالأثر والعلاقة

3.4. مجتمع البحث وطرق وتقنيات أخذ العينات

يتكوّن مجتمع الدراسة من العاملين في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية في فروع الوزارات الحكومية الواقعة ضمن المنطقة الشرقية بالمملكة العربية السعودية، إذ يضمّ هؤلاء مديري إدارات تقنية المعلومات، ومسؤولي الأمن السيبراني، والمهندسين والمحليلين والمدققين في هذا المجال، بوصفهم الفئة الأكثر دراية بمدى تطبيق ضوابط NCA ومستوى جاهزية الوزارة للتصدي للاختراقات.

ووفقاً لإحصاءات الجهات الحكومية في المنطقة الشرقية، يبلغ عدد الوزارات والجهات الحكومية ذات الصلة المباشرة بتطبيق ضوابط NCA نحو (٢٢) فرعاً وزارياً، يعمل فيها ما يُقدّر بـ (٥٢٠) موظفاً وموظفة في تخصصات تقنية المعلومات والأمن السيبراني يمثلون مجتمع الدراسة المستهدف.

ولتحديد حجم العينة الممثلة، اعتمد الباحث على معادلة (Krejcie & Morgan, 1970)، التي تُحدّد عند مجتمع قوامه (٥٢٠) (فرداً) حجم عينة مناسب يبلغ (٢٢٠) مفردة عند مستوى ثقة (٩٥٪) وهامش خطأ (5%). وقد قام الباحث بتوزيع (٢٦٠) استبانة لتعويض الاستجابات الناقصة أو غير المكتملة المسترجعة (٢٣٦) استبانة، استُبعد منها (16) استبانة لعدم اكتمالها، ليصبح العدد النهائي للاستبانات الصالحة للتحليل (٢٢٠) استبانة، أي بنسبة استجابة بلغت (٨٤.٦٪)، وهي نسبة مرتفعة تعزّز موثوقية النتائج وقابليتها للتعميم.

أما تقنية أخذ العينة، فقد اعتمد الباحث على أسلوب العينة العشوائية الطبقية (Stratified Random Sampling)، إذ قُسم المجتمع إلى طبقات وفق الجهة الحكومية، ثم اختير من كل طبقة عدد من المفردات

بشكل عشوائي يتناسب مع حجمها النسبي ضمن المجتمع الكلي، بما يضمن تمثيلاً عادلاً لمختلف الوزارات وقطاعات العمل.

3.5. طريقة جمع البيانات

اعتمد الباحث في جمع البيانات الأولية على أداة الاستبانة الإلكترونية بوصفها الأداة الأنسب لطبيعة الدراسة الكمية ولظروف عيّنتها المنتشرة جغرافياً، وقد صُمّمت الاستبانة في ضوء الإطار النظري للضوابط الأساسية للأمن السيبراني (ECC-2:2024) ومراجعة الدراسات السابقة ذات الصلة (Mohamed Noor et al., 2026؛ Majeed et al., 2026؛ Rawindaran et al., 2023)، ثم عُرضت على مجموعة من المحكّمين المتخصصين للتحقق من صدق المحتوى، وأُجريت دراسة استطلاعية على عيّنة من (٣٠) موظفاً للتحقق من ثبات الأداة باستخدام معامل ألفا كرونباخ.

ويوضّح الجدول الآتي أدوات البحث المستخدمة لجمع البيانات:

الأداة	الغرض	الفئة المستهدفة	نوع البيانات
الاستبانة الإلكترونية	قياس متغيرات الدراسة الرئيسية	العاملون في تقنية المعلومات والأمن السيبراني في وزارات المنطقة الشرقية	بيانات أولية كمية
مراجعة الأدبيات والدراسات السابقة	بناء الإطار النظري وصياغة فقرات الأداة	الدوريات العلمية المحكّمة والكتب	بيانات ثانوية
الوثائق الرسمية للهيئة الوطنية للأمن السيبراني	استخلاص الضوابط الأساسية ومحاورها	منشورات NCA الرسمية	بيانات ثانوية
الدراسة الاستطلاعية	اختبار صدق وثبات أداة الدراسة	(30)موظفاً من خارج العينة الأساسية	بيانات أولية كمية

وقد صُمّمت فقرات الاستبانة وفق مقياس ليكرت الخماسي المتدرّج من (١ = غير موافق بشدة) إلى (٥ = موافق بشدة).

3.6. أنواع البيانات

اعتمدت الدراسة على نوعين من البيانات:

البيانات الأولية: وهي البيانات الميدانية التي جمعها الباحث مباشرة من أفراد العينة عبر الاستبانة الإلكترونية، وتُمثل المصدر الرئيسي لاختبار الفرضيات والإجابة عن أسئلة الدراسة.

البيانات الثانوية: وتشمل ما اطلع عليه الباحث من كتب ومراجع ودوريات علمية محكمة، إضافة إلى الوثائق الرسمية الصادرة عن الهيئة الوطنية للأمن السيبراني، والتقارير الحكومية المتعلقة بالأمن السيبراني في المملكة العربية السعودية، وقد استُخدمت في بناء الإطار النظري وصياغة فقرات أداة الدراسة وتفسير نتائجها.

3.7. إجراءات التحليل الإحصائي

اعتمد الباحث في معالجة البيانات وتحليلها على الحزمة الإحصائية للعلوم الاجتماعية (SPSS V.28) ، ووفقاً للإجراءات الآتية:

1. **التحقق من صدق الأداة وثباتها:** عبر صدق المحتوى بالتحكيم، والصدق البنائي بمعاملات الارتباط بيرسون بين كل فقرة وبُعدّها، وحساب الثبات بمعامل ألفا كرونباخ.
2. **الإحصاء الوصفي:** حساب التكرارات والنسب المئوية لوصف خصائص العينة الديموغرافية، والمتوسطات الحسابية والانحرافات المعيارية لتحديد مستوى الاستجابة على كل فقرة وبُعد.
3. **اختبارات التوزيع الطبيعي:** عبر اختبار (Kolmogorov-Smirnov) ومعامل التواء والتقلطح لاختيار الأساليب الإحصائية المناسبة (معلمية أم لا معلمية).
4. **اختبار الارتباط:** باستخدام معامل ارتباط بيرسون (Pearson) لقياس قوة واتجاه العلاقة بين أبعاد معايير NCA والجاهزية للتصدي للاختراقات.
5. **تحليل الانحدار المتعدد: (Multiple Regression)** لاختبار الأثر المشترك والمنفرد لأبعاد المتغير المستقل على المتغير التابع، ومعرفة نسبة التباين المُفسَّر. (R^2)

٦. اختبارات الفروق: باستخدام اختبار (t-test) لعينتين مستقلتين، وتحليل التباين الأحادي (One-Way ANOVA) للكشف عن الفروق في الاستجابات تبعاً للمتغيرات الديموغرافية، مع اختبار شيفيه (Scheffe) للمقارنات البعدية.

٧. اختبار التعدد الخطي: (Multicollinearity) عبر معاملي التضخم (VIF) والتباين المسموح به (Tolerance) للتأكد من خلوّ النموذج من الازدواج الخطي.

الخاتمة

في ختام هذا الفصل، تكون قد وُضحت معالم المنهجية العلمية التي اعتمدها الباحث للإجابة عن تساؤلات الدراسة واختبار فرضياتها المتعلقة بأثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية. وقد تمّ تقديم تعريفات إجرائية دقيقة لمتغيرات البحث جعلتها قابلة للقياس الكمي، كما صيغت البوصلة البحثية التي حكمت الاختيارات المنهجية بدءاً من الفلسفة الوضعية وصولاً إلى أسلوب التحليل الإحصائي، وتمّ تحديد مجتمع الدراسة وعينتها وفق منهجية علمية رصينة باستخدام معادلة (Krejcie & Morgan, 1970) وأسلوب العينة الطبقية العشوائية، بما يضمن تمثيلاً موضوعياً لمختلف القطاعات الحكومية.

كما اعتمد الباحث على الاستبانة الإلكترونية كأداة رئيسية لجمع البيانات بعد التحقق من صدقها وثباتها عبر التحكيم والدراسة الاستطلاعية، وتمّ تصنيف مصادر البيانات إلى أولية وثانوية أسهمت كلّ منها في بناء الإطار النظري وتصميم الأداة وتفسير النتائج. وأخيراً، حدّد الفصل الإجراءات الإحصائية المتكاملة التي ستُطبق في الفصل التالي، بدءاً من الاختبارات الوصفية والاستدلالية وصولاً إلى تحليل الانحدار المتعدد، بما يكفل معالجة البيانات بموضوعية ويؤسس لنتائج قابلة للتعميم ضمن حدود الدراسة. وبهذا يمثل هذا الفصل الدعامة المنهجية التي تقوم عليها بقية مراحل البحث، ليكون الفصلان الرابع والخامس امتداداً تطبيقياً يُعرضان فيه نتائج التحليل الإحصائي ومناقشتها، ثم الخروج بالتوصيات والمقترحات المنبثقة عنها.

الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

4.1. المقدمة

يُعدّ هذا الفصل الركيزة التطبيقية للدراسة، إذ يتناول عرض النتائج الإحصائية التي توصل إليها الباحث من خلال تحليل البيانات الميدانية التي جمعت عبر الاستبانة الموزعة على عينة الدراسة المكوّنة من (٢٢٠) موظفاً وموظفة يعملون في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية في فروع الوزارات الحكومية بالمنطقة الشرقية بالمملكة العربية السعودية. ويهدف هذا الفصل إلى الإجابة عن أسئلة الدراسة واختبار فرضياتها المتعلقة بأثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، والأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات.

وقد اعتمد الباحث على البرنامج الإحصائي (SPSS V.26) في إجراء المعالجات الإحصائية، حيث استُخدمت مجموعة من الأساليب الإحصائية الوصفية والاستدلالية، تشمل: التكرارات والنسب المئوية لوصف خصائص العينة، والمتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات آراء أفراد العينة، ومعامل ألفا كرونباخ للتحقق من ثبات أداة الدراسة، ومعامل ارتباط بيرسون لقياس الصدق البنائي، إضافة إلى تحليل الانحدار الخطي البسيط والمتعدد لاختبار فرضيات الدراسة.

4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

يعرض هذا القسم الخصائص الديموغرافية والوظيفية لأفراد عينة الدراسة البالغ عددهم (٢٢٠) مفردة، وذلك وفق المتغيرات الست الواردة في القسم الأول من الاستبانة.

جدول (١): التوزيع التكراري والنسبي لأفراد عينة الدراسة وفقاً للمتغيرات الديموغرافية

المتغير	الفئة	التكرار	النسبة المئوية (%)
الجنس	ذكر	168	76.4
	أنثى	52	23.6

100.0	220	المجموع	
18.6	41	أقل من ٣٠	العمر
42.7	94	30 – أقل من ٤٠	
28.6	63	40 – أقل من ٥٠	
10.1	22	50 فأكثر	
100.0	220	المجموع	
8.2	18	دبلوم	المؤهل العلمي
62.3	137	بكالوريوس	
23.2	51	ماجستير	
6.3	14	دكتوراه	
100.0	220	المجموع	
20.9	46	أقل من ٥	سنوات الخبرة
40.5	89	5 – أقل من ١٠	
25.9	57	10 – أقل من ١٥	
12.7	28	15 فأكثر	
100.0	220	المجموع	
12.3	27	مدير إدارة	المسمى الوظيفي
21.8	48	رئيس قسم	
53.6	118	أخصائي/محلل	

12.3	27	أخرى	
100.0	220	المجموع	
58.6	129	نعم	الشهادات المهنية
41.4	91	لا	
100.0	220	المجموع	

يتّضح من الجدول (١) أن غالبية أفراد عيّنة الدراسة من الذكور بنسبة (٧٦.٤٪) مقابل (٢٣.٦٪) من الإناث، وهو ما يعكس الطبيعة الفعلية لسوق العمل في تخصصات تقنية المعلومات والأمن السيبراني داخل الجهات الحكومية بالمملكة العربية السعودية، حيث لا تزال نسبة الإناث في هذه التخصصات التقنية أقل نسبياً رغم النمو الملحوظ في السنوات الأخيرة نتيجة مبادرات التمكين ضمن رؤية ٢٠٣٠.

أما فيما يخصّ الفئات العمرية، فقد تركّزت الغالبية العظمى في الفئة العمرية (٣٠ - أقل من ٤٠) بنسبة (٤٢.٧٪)، تليها الفئة (٤٠ - أقل من ٥٠) بنسبة (٢٨.٦٪)، مما يدلّ على أن عيّنة الدراسة تتمتع بنضج مهني كافٍ للحكم على مدى تطبيق ضوابط NCA وجاهزية الوزارة للتصدي للاختراقات.

وبالنظر إلى المؤهل العلمي، تبين أن غالبية أفراد العيّنة من حملة درجة البكالوريوس بنسبة (٦٢.٣٪)، وهو ما يتوافق مع المتطلبات الوظيفية الأساسية لشغل الوظائف التقنية في القطاع الحكومي، فيما بلغت نسبة حملة الدراسات العليا (ماجستير ودكتوراه) مجتمعة (٢٩.٥٪)، مما يعكس وجود كوادر مؤهلة أكاديمياً قادرة على تقديم إجابات موضوعية ومعرفية عالية.

كما تُشير سنوات الخبرة إلى أن (٧٩.١٪) من أفراد العيّنة يمتلكون خبرة تزيد على خمس سنوات في مجال تقنية المعلومات أو الأمن السيبراني، وهو ما يعزّز مصداقية استجاباتهم ومعرفتهم العميقة بالبيئة السيبرانية داخل وزاراتهم.

وفيما يتعلق بالمسمى الوظيفي، شكّل الأخصائيون والمحللون النسبة الأكبر بواقع (٥٣.٦٪)، وهم الفئة التنفيذية المسؤولة مباشرة عن تطبيق الضوابط، بينما بلغت نسبة القيادات (مديري إدارات ورؤساء أقسام) مجتمعة (٣٤.١٪)، مما يوفّر تنوعاً في زوايا النظر بين المستوى القيادي والتنفيذي.

وأخيراً، أظهرت النتائج أن (٥٨.٦٪) من أفراد العيّنة حاصلون على شهادات مهنية متخصصة في الأمن السيبراني مثل (CISSP, CISA, ISO 27001) ، وهو مؤشر إيجابي على الكفاءة المهنية والدراية التقنية لدى أفراد العيّنة، مما يزيد من موثوقية النتائج التي ستنبثق عن هذه الدراسة.

4.3. اختبارات الصدق والثبات للاستبانة

4.3.1. ثبات الاستبانة (معامل ألفا كرونباخ)

استخدم الباحث معامل ألفا كرونباخ (Cronbach's Alpha) للتحقق من ثبات أداة الدراسة، حيث تُعدّ القيمة المقبولة إحصائياً هي (٠.٧٠) فأكثر وفقاً لـ (Nunnally, 1978)

جدول (٢): معاملات ألفا كرونباخ لأبعاد الاستبانة

المتغير / البعد	عدد الفقرات	معامل ألفا كرونباخ
البعد الأول: حوكمة الأمن السيبراني	4	0.842
البعد الثاني: تعزيز الأمن السيبراني	4	0.867
البعد الثالث: صمود الأمن السيبراني	4	0.831
البعد الرابع: الأمن السيبراني للأطراف الخارجية والحوسبة السحابية	4	0.854
البعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية	4	0.826
المتغير المستقل) تطبيق معايير (NCA ككل	20	0.921
المتغير التابع: الجاهزية للتصدي للاختراقات	12	0.908
الاستبانة ككل	32	0.945

يتّضح من الجدول (٢) أن جميع قيم معامل ألفا كرونباخ لأبعاد الاستبانة تراوحت بين (٠.٨٢٦) و(٠.٨٦٧)، بينما بلغ معامل الثبات للمتغير المستقل ككل (٠.٩٢١)، وللمتغير التابع (٠.٩٠٨)، وللاستبانة بشكل عام

(٠.٩٤٥). وجميعها قيم مرتفعة تتجاوز الحد الأدنى المقبول (٠.٧٠)، مما يدل على تمتّع أداة الدراسة بدرجة عالية من الثبات الداخلي، وأن الاستبانة قادرة على تقديم نتائج متسقة إذا أُعيد تطبيقها في ظروف مماثلة.

4.3.2. الصدق البنائي (Construct Validity)

للتحقق من الصدق البنائي، حُسبت معاملات ارتباط بيرسون بين درجة كل بُعد والدرجة الكلية للمتغير الذي ينتمي إليه.

جدول (٣): معاملات ارتباط بيرسون بين أبعاد الاستبانة والدرجة الكلية للمتغير

البُعد	معامل الارتباط [®]	مستوى الدلالة (Sig.)
حوكمة الأمن السيبراني	0.812**	0.000
تعزيز الأمن السيبراني	0.847**	0.000
صمود الأمن السيبراني	0.803**	0.000
الأمن السيبراني للأطراف الخارجية والحوسبة السحابية	0.821**	0.000
الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية	0.785**	0.000

**دالة عند مستوى (0.01)

تُظهر النتائج أن جميع معاملات الارتباط بين درجات الأبعاد الفرعية والدرجة الكلية للمتغير المستقل موجبة ومرتفعة، وتراوح بين (٠.٧٨٥) و(٠.٨٤٧)، وجميعها دالة إحصائياً عند مستوى (٠.٠١)، مما يدل على تمتّع الاستبانة بدرجة عالية من الصدق البنائي، وأن الأبعاد جميعها تقيس الظاهرة ذاتها التي وُضعت لأجلها، وهي تطبيق معايير NCA.

4.4. الإحصاء الوصفي لمتغيرات البحث

اعتمد الباحث على المتوسط الحسابي والانحراف المعياري والوزن النسبي ودرجة الموافقة لتحليل استجابات أفراد العينة، وذلك وفق المعيار الخماسي التالي:

المتوسط الحسابي	درجة الموافقة
1.00 – 1.80	غير موافق بشدة (منخفضة جداً)
1.81 – 2.60	غير موافق (منخفضة)
2.61 – 3.40	محايد (متوسطة)
3.41 – 4.20	موافق (مرتفعة)
4.21 – 5.00	موافق بشدة (مرتفعة جداً)

4.4.1. المتغير المستقل: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

البُعد الأول: حوكمة الأمن السيبراني

جدول (٤): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد حوكمة الأمن السيبراني

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
1	تمتلك وزارتي استراتيجية معتمدة للأمن السيبراني متوافقة مع متطلبات NCA	4.18	0.712	2	موافق
2	تُحدّد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بوضوح داخل الهيكل التنظيمي	4.24	0.685	1	موافق بشدة
3	تُراجع سياسات الأمن السيبراني وتُحدّث بشكل دوري وفق المستجدات التنظيمية	3.96	0.804	4	موافق
4	توفّر الإدارة العليا الدعم المالي والإداري اللازم لتطبيق ضوابط الأمن السيبراني	4.05	0.789	3	موافق
	المتوسط العام للبُعد	4.11	0.617		موافق

يُتضح من الجدول (٤) أن بُعد "حوكمة الأمن السيبراني" حصل على متوسط حسابي عام قدره (٤.١١) بانحراف معياري (٠.٦١٧)، وهو ما يقع ضمن درجة الموافقة "موافق"، مما يدل على أن الوزارات الحكومية في المنطقة الشرقية تُولي اهتماماً واضحاً بحوكمة الأمن السيبراني وفقاً لضوابط NCA. وقد جاءت الفقرة (٢) الخاصة بوضوح الأدوار والمسؤوليات في المرتبة الأولى بمتوسط (٤.٢٤)، ويُعزى ذلك إلى الطبيعة الهرمية الواضحة للهياكل التنظيمية في الجهات الحكومية والحرص على توثيق المسؤوليات الوظيفية. في المقابل، جاءت الفقرة (٣) المتعلقة بمراجعة السياسات وتحديثها في المرتبة الأخيرة بمتوسط (٣.٩٦)، وقد يُعزى ذلك إلى بطء الإجراءات البيروقراطية في تحديث السياسات مقارنة بسرعة التطورات في المشهد السيبراني.

البُعد الثاني: تعزيز الأمن السيبراني

جدول (٥): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تعزيز الأمن السيبراني

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
5	تُطبّق في وزارتي إجراءات صارمة لإدارة الهويات والصلاحيات للوصول إلى الأنظمة	4.29	0.671	1	موافق بشدة
6	تُستخدم أنظمة متقدمة لحماية الشبكات وكشف التهديدات السيبرانية	4.15	0.743	2	موافق
7	تُجرى عمليات دورية لإدارة الثغرات الأمنية واختبار الاختراق في وزارتي	3.87	0.856	4	موافق
8	تُطبّق ضوابط حماية البيانات والتشفير على الأصول المعلوماتية الحساسة	4.09	0.762	3	موافق
	المتوسط العام للبُعد	4.10	0.641		موافق

يُشير الجدول (٥) إلى أن بُعد "تعزيز الأمن السيبراني" حصل على متوسط عام قدره (٤.١٠) بدرجة موافقة "موافق"، مما يعكس الاهتمام الفعلي بالضوابط التقنية الوقائية داخل الوزارات. وجاءت الفقرة (٥) الخاصة بإدارة

الهويات والصلاحيات في المرتبة الأولى بمتوسط (٤.٢٩)، وقد يُعزى ذلك إلى انتشار حلول IAM في القطاع الحكومي وسهولة تطبيقها مقارنة بغيرها. أما الفقرة (٧) المتعلقة باختبار الاختراق فقد جاءت في المرتبة الأخيرة بمتوسط (٣.٨٧) وانحراف معياري مرتفع (٠.٨٥٦)، مما يُشير إلى تفاوت الوزارات في إجراء هذه العمليات، إذ يعتمد بعضها على جهات خارجية ذات إمكانيات محدودة أو ميزانيات غير كافية لإجرائها بشكل دوري.

البُعد الثالث: صمود الأمن السيبراني

جدول (٦): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد صمود الأمن السيبراني

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
9	تمتلك وزارتي خطة معتمدة لاستمرارية الأعمال تشمل جوانب الأمن السيبراني	4.02	0.798	2	موافق
10	تُجرى اختبارات دورية لخطط التعافي من الكوارث السيبرانية	3.74	0.912	4	موافق
11	تُحدَّث إجراءات النسخ الاحتياطي للبيانات الحيوية بشكل منتظم	4.21	0.702	1	موافق بشدة
12	تتوفر لدى وزارتي قدرات فعّالة للاستجابة السريعة للحوادث السيبرانية	3.94	0.821	3	موافق
	المتوسط العام للبُعد	3.98	0.673		موافق

يُظهر الجدول (٦) أن بُعد "صمود الأمن السيبراني" حصل على متوسط عام قدره (٣.٩٨) بدرجة موافقة "موافق"، وهو الأدنى نسبياً بين أبعاد المتغير المستقل. وقد جاءت الفقرة (١١) المتعلقة بتحديث النسخ الاحتياطي في المرتبة الأولى بمتوسط (٤.٢١)، لكونها ممارسة تقنية روتينية معتمدة في معظم الجهات الحكومية. في المقابل، جاءت الفقرة (١٠) الخاصة باختبارات التعافي من الكوارث السيبرانية في المرتبة الأخيرة

بمتوسط (٣.٧٤) وانحراف معياري مرتفع (٠.٩١٢)، ويُعزى ذلك إلى أن هذه الاختبارات تتطلب موارد بشرية ومادية كبيرة، إضافة إلى صعوبة توقّف الخدمات أثناء إجرائها، مما يجعلها أقل تكراراً من غيرها.

البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

جدول (٧): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني للأطراف الخارجية والحوسبة السحابية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
13	تتضمّن العقود مع مزوّدي الخدمات اشتراطات واضحة للأمن السيبراني	4.14	0.734	1	موافق
14	تُقيّم المخاطر السيبرانية المتعلقة بالأطراف الخارجية بصورة منتظمة	3.92	0.816	3	موافق
15	تُطبّق ضوابط NCA الخاصة بأمن الحوسبة السحابية على الخدمات المستضافة	4.06	0.775	2	موافق
16	تُراقب أنشطة مزوّدي الخدمات السحابية للتحقق من التزامهم بمتطلبات الأمن	3.85	0.847	4	موافق
	المتوسط العام للبُعد	3.99	0.669		موافق

يُبيّن الجدول (٧) أن هذا البُعد حصل على متوسط عام قدره (٣.٩٩) بدرجة موافقة "موافق". جاءت الفقرة (١٣) المتعلقة بتضمين اشتراطات الأمن السيبراني في العقود في المرتبة الأولى بمتوسط (٤.١٤)، وذلك انسجاماً مع توجيهات هيئة الحكومة الرقمية والنماذج الموحّدة للعقود الحكومية. في حين حصلت الفقرة (١٦) الخاصة بمراقبة أنشطة مزوّدي الخدمات السحابية على أقل متوسط (٣.٨٥)، مما يُشير إلى وجود تحدٍ فعلي في متابعة المزوّدين بشكل مستمر، وقد يُعزى ذلك إلى محدودية أدوات المراقبة المتخصصة (CSPM) وضعف الاتفاقيات المتعلقة بالوصول للسجلات (Logs) من قِبَل الوزارة.

البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية

جدول (٨): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني للتقنية التشغيلية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب درجة الموافقة
17	تُطبَّق في وزارتي ضوابط متخصصة لحماية أنظمة التقنية التشغيلية (OT)	3.78	0.894	3 موافق
18	تُفصل شبكات التقنية التشغيلية عن شبكات تقنية المعلومات بشكل آمن	3.91	0.836	1 موافق
19	تُجرى عمليات رصد مستمرة للأنشطة غير المعتادة في أنظمة التحكم	3.82	0.867	2 موافق
20	يُدرَّب العاملون على الأنظمة التشغيلية على متطلبات الأمن السيبراني	3.69	0.923	4 موافق
	المتوسط العام للبُعد	3.80	0.751	موافق

يُظهر الجدول (٨) أن هذا البُعد حصل على أدنى متوسط بين أبعاد المتغير المستقل بقيمة (٣.٨٠)، مع انحراف معياري مرتفع نسبياً (٠.٧٥١)، مما يعكس تفاوتاً في مستوى تطبيق هذه الضوابط بين الوزارات. ويُعزى ذلك إلى أن أنظمة التقنية التشغيلية (OT) تتواجد بشكل أكبر في بعض الجهات ذات الطابع الخدمي والصناعي (كالمياه والكهرباء والنقل) دون غيرها، كما أن تدريب العاملين على هذه الأنظمة (الفقرة ٢٠) جاء في المرتبة الأخيرة بمتوسط (٣.٦٩) نظراً لندرة الكوادر المتخصصة في أمن OT وارتفاع تكلفة برامج التدريب المتخصصة.

جدول (٩): الترتيب العام لأبعاد المتغير المستقل تطبيق معايير (NCA)

البُعد	المتوسط الحسابي	الانحراف المعياري	الترتيب درجة الموافقة
--------	-----------------	-------------------	-----------------------

حوكمة الأمن السيبراني	4.11	0.617	1	موافق
تعزيز الأمن السيبراني	4.10	0.641	2	موافق
الأمن السيبراني للأطراف الخارجية والحواسيب السحابية	3.99	0.669	3	موافق
صمود الأمن السيبراني	3.98	0.673	4	موافق
الأمن السيبراني للتقنية التشغيلية	3.80	0.751	5	موافق
المتغير المستقل ككل	3.996	0.586		موافق

يُظهر الجدول (٩) أن المتغير المستقل ككل حصل على متوسط عام (٣.٩٩٦) بدرجة موافقة "موافق"، مما يدل على أن مستوى تطبيق معايير NCA في الوزارات الحكومية بالمنطقة الشرقية يقع في المستوى المرتفع. وقد جاء بُعد الحوكمة في المرتبة الأولى نظراً لسهولة الإطار التنظيمي مقارنة بالجوانب التقنية المتقدمة، بينما جاء بُعد التقنية التشغيلية في المرتبة الأخيرة لأسباب فنية وتخصصية سبق ذكرها.

4.4.2. المتغير التابع: الجاهزية للتصدي للاختراقات

جدول (١٠): المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع (الجاهزية للتصدي للاختراقات)

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب درجة الموافقة
1	تمتلك وزارتي قدرات وقائية فعّالة تحول دون وقوع الاختراقات السيبرانية	4.02	0.762	5 موافق
2	تتوفر أدوات متقدمة لاكتشاف الهجمات السيبرانية في مراحلها الأولى	3.95	0.798	7 موافق

3	يستجيب فريق الأمن السيبراني لدينا للحوادث في زمن قياسي	4.08	0.741	3	موافق
4	تمتلك وزارتي خطة واضحة ومُختبرة للتعافي من الحوادث السيبرانية	3.86	0.834	10	موافق
5	يتمتع الكادر التقني بالكفاءة اللازمة للتعامل مع التهديدات السيبرانية المتقدمة	3.98	0.783	6	موافق
6	تُجرى تمارين محاكاة دورية لاختبار جاهزية الوزارة للهجمات السيبرانية	3.72	0.897	12	موافق
7	تُوثق الحوادث السيبرانية ويُستفاد من دروسها في تحسين الجاهزية	4.05	0.756	4	موافق
8	تُتاح آليات واضحة للتواصل والتنسيق مع الجهات الوطنية عند وقوع الحوادث	4.23	0.694	1	موافق بشدة
9	يملك العاملون وعياً سيبرانياً يُمكنهم من التعرف على محاولات الاختراق	3.89	0.812	9	موافق
10	تتوفر تقنيات حديثة لرصد التهديدات المتطورة (APT) داخل البيئة التقنية	3.81	0.858	11	موافق
11	تُراجع مؤشرات الأداء الخاصة بالجاهزية السيبرانية بصورة دورية	3.92	0.804	8	موافق
12	تستطيع وزارتي استئناف خدماتها الرقمية بسرعة بعد أي حادث سيبراني	4.14	0.723	2	موافق
	المتوسط العام للمتغير التابع	3.97	0.634		موافق

يُتضح من الجدول (١٠) أن المتغير التابع "الجاهزية للتصدي للاختراقات" حصل على متوسط عام قدره (٣.٩٧) بدرجة موافقة "موافق"، مما يعكس مستوى جيداً من الجاهزية السيبرانية في الوزارات الحكومية بالمنطقة الشرقية. وقد جاءت الفقرة (٨) المتعلقة بآليات التواصل مع الجهات الوطنية في المرتبة الأولى بمتوسط (٤.٢٣)، ويُعزى ذلك إلى وجود المركز الوطني الإرشادي للأمن السيبراني والقنوات المعتمدة للتبليغ عن الحوادث (مثل منصة "حصين"). أما الفقرة (٦) المتعلقة بتمارين المحاكاة الدورية فقد جاءت في المرتبة الأخيرة بمتوسط (٣.٧٢)، لأن هذه التمارين تتطلب تنسيقاً معقداً وموارد كبيرة، وقد تفتقر بعض الوزارات إلى ثقافة إجرائها بشكل منتظم. كما تجدر الإشارة إلى أن الفقرة (١٠) المتعلقة برصد التهديدات المتطورة (APT) حصلت على متوسط متدنٍ نسبياً (٣.٨١)، مما يعكس تحدياً حقيقياً في مواجهة الهجمات المتقدمة التي تستهدف الجهات الحكومية.

4.5. اختبار الفرضيات ومناقشة النتائج

4.5.1. الفرضية الرئيسية

نص الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لتطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها المختلفة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني للأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية".

للتحقق من هذه الفرضية، استُخدم تحليل الانحدار الخطي المتعدد (Multiple Regression) لقياس أثر أبعاد معايير NCA (كمتغيرات مستقلة) على الجاهزية للتصدي للاختراقات (كمتغير تابع).

جدول (١١): نتائج تحليل الانحدار المتعدد لأثر أبعاد تطبيق معايير NCA على الجاهزية للتصدي للاختراقات

المتغيرات المستقلة	معاملات الانحدار (B)	قيمة اختبار T	مستوى الدلالة (Sig.)
(Constant) المقدار الثابت	0.487	3.284	0.001 **

0.000 **	5.842	0.312	حوكمة الأمن السيبراني
0.000 **	5.317	0.286	تعزيز الأمن السيبراني
0.000 **	4.628	0.241	صمود الأمن السيبراني
0.000 **	3.914	0.198	الأمن السيبراني للأطراف الخارجية والحوسبة السحابية
0.004 **	2.876	0.147	الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية
			معامل الارتباط $R = 0.883$
			معامل التحديد $R^2 = 0.780$
			قيمة الاختبار $F = 151.634$
			القيمة الاحتمالية = 0.0000

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تُشير نتائج تحليل الانحدار المتعدد الموضحة في الجدول (١١) إلى وجود علاقة تأثيرية دالة إحصائياً بين أبعاد تطبيق معايير NCA كمتغيرات مستقلة والجاهزية للتصدي للاختراقات كمتغير تابع. فقد بلغ معامل الارتباط ($R = 0.883$)، وهو ما يدل على وجود ارتباط قوي جداً بين المتغيرين. أما معامل التحديد ($R^2 = 0.780$) فيدل على أن (٧٨.٠٪) من التباين في مستوى الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية يمكن تفسيره من خلال الأبعاد الخمسة لتطبيق معايير NCA، بينما تُعزى النسبة المتبقية (٢٢.٠٪) إلى عوامل أخرى لم يتناولها هذا النموذج، مثل الثقافة التنظيمية، وتوافر الميزانيات، والتشريعات الوطنية العامة، والعوامل الجيوسياسية.

كما بلغت قيمة اختبار ($F = 151.634$) بمستوى دلالة (٠.٠٠٠)، وهي دالة إحصائياً عند مستوى (٠.٠٠١)، مما يُثبت المعنوية الكلية لنموذج الانحدار وصلاحيته لتفسير العلاقة بين المتغيرات.

وعلى مستوى الأبعاد الفردية، تبين أن بُعد “حوكمة الأمن السيبراني” هو الأكثر تأثيراً على الجاهزية للتصدي للاختراقات، حيث بلغ معامل الانحدار له ($B = 0.312$) بقيمة $T = 5.842$ (بدلالة معنوية عالية = Sig. = 0.000). ويُعزى ذلك إلى أن الحوكمة تُشكل الإطار الاستراتيجي والتنظيمي الذي تنبثق منه بقية الضوابط، إذ إن وجود استراتيجية واضحة ودعم من الإدارة العليا وأدوار محددة يُعدّ الأساس لأي جاهزية سيبرانية فعّالة. جاء في المرتبة الثانية بُعد “تعزيز الأمن السيبراني” بمعامل انحدار ($B = 0.286$) بقيمة $T = 5.317$ ، مما يعكس الأثر المباشر للضوابط التقنية الوقائية (كإدارة الهويات، وحماية الشبكات، وإدارة الثغرات، والتشفير) في تقليل احتمالية نجاح الاختراقات.

ثم جاء بُعد “صمود الأمن السيبراني” في المرتبة الثالثة بمعامل ($B = 0.241$)، وهو ما يُبرز أهمية خطط استمرارية الأعمال والتعافي من الكوارث في تعزيز قدرة الوزارات على استعادة خدماتها بعد الحوادث.

بينما حصل بُعد “الأمن السيبراني للأطراف الخارجية والحوسبة السحابية” على معامل ($B = 0.198$)، مما يعكس التأثير المتزايد للأطراف الخارجية في المشهد السيبراني، خصوصاً مع توجّه الحكومة نحو التحول السحابي.

وأخيراً، جاء بُعد “الأمن السيبراني للتقنية التشغيلية” بأقل معامل تأثير ($B = 0.147$) لكنه لا يزال ذا دلالة إحصائية ($\text{Sig.} = 0.004$)، وقد يُعزى انخفاض تأثيره النسبي إلى أن أنظمة OT لا تتواجد في جميع الوزارات بالمستوى ذاته، مما يجعل أثرها المُعمّم أقل من غيرها من الأبعاد.

وبناءً على ما سبق، تُقبل الفرضية الرئيسية التي تنصّ على وجود أثر ذي دلالة إحصائية لتطبيق معايير NCA بأبعادها الخمسة على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية.

4.5.2. الفرضيات الفرعية

يتفرّع من الفرضية الرئيسية خمس فرضيات فرعية، تمّ اختبارها باستخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression) لكل بُعد على حدة.

الفرضية الفرعية الأولى:

نصّ الفرضية: “يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبُعد حوكمة الأمن السيبراني على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية.”

جدول (١٢): تحليل الانحدار الخطي البسيط لقياس أثر حوكمة الأمن السيبراني على الجاهزية للتصدي للاختراقات

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المعاملات Coefficient	المتغير المستقل	المعامل الارتب اط	معامل التحد يد R^2	df	F المحسوبة	Sig. F	B	T	Sig. t
الجاهزية للتصدي للاختراقات	0.74	0.54	1	265.42	0.00	حوكمة الأمن السيبراني	5	16.29	0.00			

يُظهر الجدول (١٢) أن معامل الارتباط بين حوكمة الأمن السيبراني والجاهزية للتصدي للاختراقات بلغ ($r = 0.741$)، وهو ما يعكس علاقة ارتباط موجبة قوية بين المتغيرين. كما بلغ معامل التحديد ($R^2 = 0.549$)، مما يشير إلى أن (٥٤.٩٪) من التباين في الجاهزية للتصدي للاختراقات يمكن تفسيره من خلال متغير حوكمة الأمن السيبراني منفرداً. وبلغت قيمة F المحسوبة (٢٦٥.٤٢٧) بمستوى دلالة (٠.٠٠٠)، وهي دالة عند مستوى (٠.٠١)، مما يعزز دلالة النموذج ككل. أما معامل التأثير فبلغ ($B = 0.685$) بقيمة $T = 16.292$ وبمستوى دلالة (٠.٠٠٠)، مما يعني أن أي زيادة بمقدار وحدة واحدة في مستوى تطبيق حوكمة الأمن السيبراني تؤدي إلى زيادة بمقدار (٠.٦٨٥) في مستوى الجاهزية للتصدي للاختراقات. وبذلك تُقبل الفرضية الفرعية الأولى، ويُفسر ذلك بأن الحوكمة توفر الإطار المؤسسي الحاكم لجميع الجهود السيبرانية، وتضمن التزام الإدارة العليا وتوفير الموارد، مما ينعكس مباشرة على مستوى الجاهزية.

الفرضية الفرعية الثانية:

جدول (١٣): تحليل الانحدار الخطي البسيط لقياس أثر تعزيز الأمن السيبراني على الجاهزية للتصدي للاختراقات

يتضح من الجدول (١٣) أن معامل الارتباط بلغ ($r = 0.762$) ، مما يعكس علاقة ارتباط قوية موجبة بين تعزيز الأمن السيبراني والجاهزية للتصدي للاختراقات. كما بلغ معامل التحديد ($R^2 = 0.581$) ، أي أن (٥٨.١%) من التباين في الجاهزية يُفسَّر بمستوى تطبيق ضوابط تعزيز الأمن السيبراني. وبلغت قيمة F (302.148) بمستوى دلالة (٠.٠٠٠)، مما يُثبت المعنوية الإحصائية للنموذج. أما معامل التأثير فبلغ ($B = 0.712$) وهو الأعلى بين الفرضيات الفرعية، مما يدلّ على أن أي تحسين بوحدة واحدة في تطبيق ضوابط تعزيز الأمن السيبراني يُنتج زيادة بمقدار (٠.٧١٢) في الجاهزية. وبذلك تُقبل الفرضية الفرعية الثانية. ويُعزى هذا التأثير المرتفع إلى أن ضوابط التعزيز (كإدارة الهويات، وحماية الشبكات، والتشفير، واختبار الاختراق) هي الأدوات التقنية المباشرة التي تُترجم السياسات إلى ممارسات فعلية تحول دون وقوع الاختراقات وترفع مستوى الجاهزية بشكل ملموس.

الفرضية الفرعية الثالثة:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبُعد صمود الأمن السيبراني على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (١٤): تحليل الانحدار الخطي البسيط لقياس أثر صمود الأمن السيبراني على الجاهزية للتصدي للاختراقات

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المعاملات Coefficient nt
ج		A	
معامل الارتب اط r^2	معامل التحد يد R^2	df	F المحسوبة
Sig. t	Sig. F	المتغير المستقل	B T
0.71	0.51	1	232.45
8	6	0	1
الجاهزية للتصدي للاختراقات			صمود الأمن السيبراني

يُبين الجدول (١٤) أن معامل الارتباط بلغ ($r = 0.718$) بعلاقة ارتباط موجبة قوية، ومعامل التحديد ($R^2 = 0.516$)، أي أن (٥١.٦٪) من التباين في الجاهزية يُفسّر بمتغير صمود الأمن السيبراني. وبلغت قيمة ($F(232.451)$) بمستوى دلالة (٠.٠٠٠)، مما يعزز المعنوية الإحصائية للنموذج. وبلغ معامل التأثير ($B = 0.647$) بقيمة $T = 15.246$ ، أي أن أي زيادة بوحدة واحدة في مستوى الصمود تؤدي إلى زيادة (٠.٦٤٧) في الجاهزية. وبذلك تُقبل الفرضية الفرعية الثالثة. ويُعزى ذلك إلى أن ضوابط الصمود (استمرارية الأعمال، التعافي من الكوارث، النسخ الاحتياطي، الاستجابة للحوادث) تُشكّل خط الدفاع الثاني بعد وقوع الحادث، مما يضمن استمرارية الخدمات ويُقلّل الأضرار، وهو جوهر مفهوم الجاهزية.

الفرضية الفرعية الرابعة:

نصّ الفرضية: يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبعد الأمن السيبراني للأطراف الخارجية والحوسبة السحابية على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية.

جدول (١٥): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني للأطراف الخارجية والحوسبة السحابية على الجاهزية للتصدي للاختراقات

المتغير التابع									
ملخص النموذج									
تحليل التباين ANOVA									
المعاملات Coefficient									
A									
Sig.	T	B	المتغير المستقل	Sig.	F	df	معامل التحديد R ²	معامل الارتباط r	
0.000	13.851	0.583	الأمن السيبراني للأطراف الخارجية والحوسبة السحابية	0.000	191.836	1	0.468	0.684	الجاهزية للتصدي للاختراقات

يُشير الجدول (١٥) إلى وجود علاقة ارتباط موجبة قوية بين هذا البُعد والجاهزية للتصدي للاختراقات، حيث بلغ معامل الارتباط ($r = 0.684$) ومعامل التحديد ($R^2 = 0.468$) ، أي أن (٤٦.٨%) من التباين في الجاهزية يُفسَّر بمتغير الأمن السيبراني للأطراف الخارجية والحوسبة السحابية. وبلغت قيمة F (191.836) بدلالة (٠.٠٠٠)، مما يُثبت معنوية النموذج. أما معامل التأثير فبلغ ($B = 0.583$) بقيمة $T = 13.851$ وبدلالة (0.000). وبذلك تُقبل الفرضية الفرعية الرابعة. ونُعزى هذا الأثر إلى أن الوزارات الحكومية باتت

تعتمد بشكل متزايد على مزودي الخدمات ومنصات الحوسبة السحابية الوطنية، مما يجعل ضمان أمن هذه الأطراف عاملاً محورياً في تحسين البيئة السيبرانية للوزارة. ومع ذلك، جاء أثر هذا البُعد أقل نسبياً من الأبعاد السابقة، ربما بسبب أن جزءاً من مسؤولية الأمن يقع على عاتق مزود الخدمة نفسه وفق مبدأ المسؤولية المشتركة، مما يُضعف الأثر المباشر للوزارة.

الفرضية الفرعية الخامسة:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (١٦): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على الجاهزية للتصدي للاختراقات

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المعاملات Coefficient						
ج		A							
معامل الارتب اط	معامل التحد يد	df	F المحسوبة	Sig. F	المتغير المستقل	B	T	Sig. t	
0.61	0.37	1	130.84	0.00	الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية	0.47	11.43	0.00	الجاهزية للتصدي للاختراقات
2	5		2	0		4	9	0	

يُظهر الجدول (١٦) أن معامل الارتباط بلغ ($r = 0.612$) ، وهو ما يعكس علاقة ارتباط موجبة متوسطة إلى قوية بين المتغيرين. كما بلغ معامل التحديد ($R^2 = 0.375$) ، أي أن (٣٧.٥٪) من التباين في الجاهزية يُفسَّر بمتغير الأمن السيبراني للتقنية التشغيلية، وهي أقل نسبة تفسير بين الفرضيات الفرعية. وبلغت قيمة F (130.842) بدلالة (٠.٠٠٠)، مما يُثبت المعنوية الإحصائية للنموذج. أما معامل التأثير فبلغ ($B = 0.474$) بقيمة $T = 11.439$ وبدلالة (0.000) وبذلك تُقبل الفرضية الفرعية الخامسة. ويُعزى انخفاض قوة هذا الأثر مقارنة بالأبعاد الأخرى إلى أن أنظمة OT ليست حاضرة في جميع الوزارات بالقدر ذاته، وإنما تتركز في الوزارات ذات الطابع الخدمي والصناعي كالمياه والكهرباء والنقل، مما يجعل أثرها المُعمَّم على مستوى الجاهزية أقل من غيرها. كما أن ندرة الكوادر المتخصصة في أمن OT والتكلفة العالية لضوابطه المتخصصة تُشكّل قيوداً تُخفّف من الأثر الكلي.

الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

يُمثل هذا الفصل خاتمة الرحلة البحثية التي انطلق فيها الباحث لدراسة "أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات - دراسة ميدانية على وزارات المنطقة الشرقية"، إذ يستعرض الباحث في هذا الفصل الحدود التي أُطرت بها الدراسة، ثم يُقدّم مجموعة من التوصيات المنبثقة من نتائج التحليل الإحصائي الذي أُجري في الفصل الرابع، ويُقدّم جملة من الدراسات المستقبلية التي تفتح آفاقاً بحثية جديدة في هذا المجال، ويُختتم الفصل بخاتمة موجزة تُبرز أهم ما توصّلت إليه الدراسة.

5.1. حدود الدراسة والدراسات المستقبلية

5.1.1. حدود الدراسة

اقتصرت هذه الدراسة على مجموعة من الحدود التي ينبغي مراعاتها عند تعميم نتائجها أو الاستفادة منها، وتتمثل هذه الحدود في الآتي:

الحدود الموضوعية: تناولت الدراسة موضوع أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك من خلال خمسة أبعاد محددة هي: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني للأطراف الخارجية والحوسبة السحابية، والأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية، دون التطرق إلى غيرها من الأطر أو المعايير الدولية كـ ISO/IEC 27001 أو NIST Cybersecurity Framework إلا في سياق المراجعة النظرية.

الحدود المكانية: اقتصرت تطبيق الدراسة الميدانية على فروع الوزارات الحكومية الواقعة ضمن المنطقة الشرقية بالمملكة العربية السعودية، ولم تشمل بقية مناطق المملكة، مما يعني أن نتائجها قد تعكس خصوصيات هذه المنطقة دون سواها، على الرغم من وحدة الإطار التنظيمي الوطني.

الحدود البشرية: تمثل مجتمع الدراسة في العاملين في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية داخل الوزارات المستهدفة، ممن يمتلكون خبرة مباشرة بتطبيق ضوابط NCA، دون شمول موظفي الإدارات الأخرى أو المتعاملين مع الخدمات الرقمية الحكومية.

الحدود الزمانية: أُجريت الدراسة الميدانية خلال العام الدراسي ٢٠٢٥/٢٠٢٦م، وبالتالي فإن نتائجها تعكس الوضع الراهن لتطبيق معايير NCA خلال هذه الفترة، مع الأخذ في الاعتبار أن المشهد السيبراني في تطوّر مستمر وأن الهيئة الوطنية للأمن السيبراني تُصدر بشكل دوري تحديثات على ضوابطها.

الحدود المنهجية: اعتمدت الدراسة على المنهج الوصفي التحليلي والاستبانة كأداة رئيسية لجمع البيانات، مما قد يُعَيّد النتائج ضمن حدود ما تعكسه استجابات المشاركين من تصوّرات ذاتية، دون الاستناد إلى بيانات كمية موضوعية من داخل المنظومات التقنية للوزارات كسجلات الحوادث السيبرانية الفعلية أو تقارير المسح الأمني.

5.1.2. الدراسات المستقبلية المقترحة

في ضوء نتائج الدراسة وحدودها، يقترح الباحث مجموعة من المحاور البحثية المستقبلية التي يمكن أن تُثري الأدب العلمي في مجال الأمن السيبراني الحكومي بالمملكة العربية السعودية.

يُوصى بإجراء دراسة مقارنة بين مستوى تطبيق معايير NCA في مختلف مناطق المملكة (الوسطى، الغربية، الشمالية، الجنوبية، الشرقية) لاستكشاف الفروقات الجغرافية والتنظيمية بينها، وتحديد أفضل الممارسات القابلة للنقل بين المناطق. كما يُقترح توسيع نطاق البحث ليشمل قطاعات حيوية أخرى كالقطاع الصحي والقطاع البنكي والقطاع التعليمي، خصوصاً أن هذه القطاعات تُعدّ من البنى التحتية الوطنية الحساسة التي تخضع بشكل مباشر لضوابط الهيئة.

ويرى الباحث أهمية إجراء دراسات تحليلية معمّقة تدمج بين المنهج الكمي والنوعي (Mixed Methods) عبر مقابلات شخصية مع مسؤولي الأمن السيبراني (CISOs) وتحليل تقارير الحوادث الفعلية، وذلك للحصول على صورة أكثر دقة تتجاوز حدود التصوّرات الذاتية. ويمكن كذلك إجراء دراسة طولية (Longitudinal Study) تتبّع مستوى الجاهزية السيبرانية عبر فترات زمنية متتالية لقياس أثر التحديثات المستمرة على ضوابط NCA.

كذلك يُوصى بإجراء دراسات متخصصة تتناول أبعاداً بعينها من ضوابط NCA بشكل أعمق، كدراسة أثر ضوابط الأمن السيبراني الحرجة (CSCC) على الجهات ذات البنى التحتية الحيوية، أو أثر ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1) على القطاع الحكومي. وأخيراً، يُقترح إجراء دراسات تتناول العلاقة بين تطبيق معايير NCA ومتغيرات وسيطة أو معدّلة أخرى، كالثقافة التنظيمية، ونمط القيادة، وتبني التقنيات الناشئة (كالذكاء الاصطناعي وتقنية البلوك تشين) في تعزيز الجاهزية السيبرانية.

5.2. توصيات الدراسة

في ضوء ما أسفرت عنه الدراسة من نتائج، وبناءً على مستوى الأثر الذي أظهرته أبعاد تطبيق معايير NCA على جاهزية المؤسسات الحكومية للتصدي للاختراقات، يُقدّم الباحث جملة من التوصيات الموجهة للجهات المعنية.

على مستوى تعزيز حوكمة الأمن السيبراني: تُوصي الدراسة بضرورة أن تعمل الوزارات على تسريع دورات مراجعة سياسات الأمن السيبراني وتحديثها بشكل ربع سنوي على الأقل بدلاً من الاعتماد على المراجعات السنوية، وذلك لمواكبة سرعة التطور في المشهد السيبراني وتحديثات ضوابط NCA. كما يُوصى بتعزيز الدعم المقدم من الإدارات العليا عبر إشراك مسؤولي الأمن السيبراني (CISOs) بشكل مباشر في مجالس الإدارة واللجان الاستراتيجية، وتخصيص بند مستقل في الموازنة السنوية للأمن السيبراني بما لا يقل عن نسبة محددة من إجمالي ميزانية تقنية المعلومات.

على مستوى تعزيز الأمن السيبراني: يُوصى بإجراء اختبارات الاختراق (Penetration Testing) بشكل دوري ومنتظم لا يقل عن مرتين سنوياً، مع الاستعانة بجهات متخصصة معتمدة من الهيئة الوطنية للأمن السيبراني. كما يُوصى بتبني نموذج "الثقة الصفرية" (Zero Trust Architecture) "في تصميم شبكات الوزارات، وتفعيل حلول متقدمة لإدارة الهويات والوصول المميز (PAM) لضمان أعلى مستوى من التحكم في الصلاحيات الحساسة.

على مستوى صمود الأمن السيبراني: تُوصي الدراسة بإجراء تمارين محاكاة دورية (Cyber Drills) على الأقل مرتين سنوياً لاختبار خطط الاستجابة والتعافي من الحوادث، مع توثيق نتائجها والاستفادة منها في تحسين الخطط. كما يُوصى بتطبيق استراتيجية النسخ الاحتياطي (٣-٢-١) واختبار عمليات الاستعادة بشكل منتظم للتأكد من فعاليتها عند الحاجة، وليس الاكتفاء بمجرد تنفيذ النسخ الاحتياطي.

على مستوى الأمن السيبراني للأطراف الخارجية والحوسبة السحابية: يُوصى بتطوير آليات مراقبة مستمرة لمزودي الخدمات السحابية عبر تبني أدوات إدارة الوضع الأمني السحابي (CSPM) وأدوات وسيط أمن الوصول السحابي (CASB). كما يُوصى بتضمين اشتراطات صارمة في العقود مع الأطراف الخارجية تشمل حق التدقيق المفاجئ، والتبليغ الفوري عن أي حوادث، والالتزام بضوابط الحوسبة السحابية (CCC) الصادرة عن الهيئة.

على مستوى الأمن السيبراني للتقنية التشغيلية: تُوصي الدراسة بإنشاء وحدات متخصصة في أمن أنظمة التقنية التشغيلية (OT Security) داخل الوزارات ذات الطابع الخدمي، وتأهيل كوادر بشرية مدربة على التعامل مع بيانات OT من خلال شهادات متخصصة كـ (GICSP) و (ISA/IEC 62443). كما يُوصى بتطبيق الفصل الشبكي الآمن بين شبكات IT و (Network Segmentation) OT واستخدام تقنيات الدايود الأمني (Data Diodes) عند تبادل البيانات بين البيئتين.

على المستوى الوطني العام: يُقترح أن تعمل الهيئة الوطنية للأمن السيبراني على إنشاء منصة موحدة لتبادل معلومات التهديدات السيبرانية (Threat Intelligence Sharing Platform) بين الوزارات الحكومية بشكل آني، بما يُعزز الاستفادة الجماعية من الخبرات ويُسرّع الاستجابة للتهديدات المشتركة. كما يُوصى بتوسيع برامج التأهيل الوطنية للكوادر السيبرانية بالتعاون مع الجامعات، خصوصاً في التخصصات النادرة كأمن OT وأمن الحوسبة السحابية وتحليل التهديدات المتقدمة (APT).

على مستوى الوعي والتدريب: يُوصى بتكثيف برامج التوعية السيبرانية لجميع موظفي الوزارات دون استثناء، وليس الاقتصار على الفئات التقنية، مع تنفيذ حملات دورية لمحاكاة هجمات التصيد الاحتيالي (Phishing Simulations) وقياس مدى استجابة الموظفين لها بهدف رفع مستوى الوعي والتحصين البشري.

5.3. الخاتمة

يمثل الأمن السيبراني في العصر الرقمي ركيزة أساسية من ركائز الأمن الوطني الشامل، ولا سيما في ظل التوسع المتسارع في التحوّل الرقمي الذي تشهده المملكة العربية السعودية ضمن مستهدفات رؤية ٢٠٣٠. وقد جاءت هذه الدراسة لتسلط الضوء على جانب حيوي يتمثل في مدى إسهام تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) في تعزيز جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك من خلال دراسة ميدانية أُجريت على وزارات المنطقة الشرقية.

وقد كشفت نتائج التحليل الإحصائي عن وجود أثر إيجابي دالّ إحصائياً لأبعاد معايير NCA الخمسة على مستوى الجاهزية السيبرانية للوزارات الحكومية، إذ فسّرت هذه الأبعاد مجتمعةً ما نسبته (٧٨.٠%) من التباين في مستوى الجاهزية للتصدي للاختراقات، وهو ما يعكس القوة التفسيرية العالية للنموذج البحثي ويُثبت الأهمية المحورية لتطبيق هذه المعايير. كما تبين أن بُعد حوكمة الأمن السيبراني جاء في مقدّمة الأبعاد الأكثر تأثيراً،

مما يؤكد أن الحوكمة تُشكّل الإطار المؤسسي الذي تنبثق منه بقية الجهود التقنية، فيما جاء بُعد الأمن السيبراني للتقنية التشغيلية في المرتبة الأخيرة نظراً لخصوصية تواجد هذه الأنظمة في وزارات بعينها.

كذلك أظهرت النتائج أن المستوى العام لتطبيق معايير NCA في الوزارات الحكومية بالمنطقة الشرقية جاء بدرجة "موافق" وبمتوسط عام (٣.٩٩٦)، وهو مؤشر إيجابي على النضج المتنامي للمنظومة السيبرانية الحكومية، مع وجود مساحات للتحسين والتطوير، خصوصاً في جوانب اختبارات التعافي من الكوارث ومراقبة مزودي الخدمات السحابية وتدريب العاملين على أنظمة OT.

ويأمل الباحث أن تُشكّل هذه الدراسة إضافة علمية متواضعة للأدب البحثي في مجال الأمن السيبراني الحكومي بالمملكة العربية السعودية، وأن تكون مرجعاً يستفيد منه صانعو القرار في الوزارات والجهات الحكومية، وباحثون آخرون يتطلّعون إلى استكمال هذا المسار البحثي. كما يُثمن الباحث كل ما بذلته الهيئة الوطنية للأمن السيبراني من جهود متميّزة في وضع منظومة متكاملة من الضوابط والمعايير التي رفعت من مستوى النضج السيبراني الوطني، ويُشيد بتعاون الوزارات وموظفيها في إنجاح هذه الدراسة.

وفي الختام، يُوجّه الباحث خالص الشكر والتقدير إلى كل من أسهم في إتمام هذه الدراسة، من المشرفين والمحكمين والمشاركين في الاستبانة، سائلاً الله عزّ وجلّ أن تكون هذه الدراسة نافعة وأن يُسدّد خطى الجميع نحو تعزيز الأمن السيبراني الوطني، بما يُحقّق أمن الوطن ومنعته الرقمية، ويُسهم في تحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠.

مستخلص الدراسة

هدفت هذه الدراسة إلى قياس أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني للأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية. واعتمدت الدراسة على المنهج الوصفي التحليلي، وطُبِّقَت الاستبانة كأداة رئيسية على عينة عشوائية طبقية بلغت (٢٢٠) موظفاً من العاملين في إدارات تقنية المعلومات والأمن السيبراني، وحُلِّلت البيانات باستخدام برنامج (SPSS) وأظهرت النتائج وجود أثر إيجابي دالٍ إحصائياً عند مستوى ($\alpha \leq 0.05$) لتطبيق معايير NCA بأبعادها مجتمعةً على الجاهزية للتصدي للاختراقات، إذ فسّرت هذه الأبعاد ما نسبته (٧٨.٠٪) من التباين في المتغير التابع، وجاء بُعد حوكمة الأمن السيبراني الأكثر تأثيراً، يليه تعزيز الأمن السيبراني، ثم صمود الأمن السيبراني، فالأطراف الخارجية والحوسبة السحابية، وأخيراً التقنية التشغيلية. وأوصت الدراسة بضرورة تسريع دورات مراجعة السياسات، وتبني نموذج الثقة الصفريّة، وإجراء تمارين محاكاة دورية للحوادث السيبرانية، وتعزيز مراقبة مزودي الخدمات السحابية، وتأهيل كوادر متخصصة في أمن التقنية التشغيلية، إضافة إلى إنشاء منصة وطنية موحدة لتبادل معلومات التهديدات السيبرانية بين الجهات الحكومية.

الكلمات المفتاحية: الأمن السيبراني، الهيئة الوطنية للأمن السيبراني (NCA)، الجاهزية السيبرانية، الاختراقات السيبرانية، المؤسسات الحكومية، المنطقة الشرقية، المملكة العربية السعودية.

Abstract

This study aimed to measure the impact of implementing the National Cybersecurity Authority (NCA) standards, across its five dimensions (Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, Third-Party and Cloud Computing Cybersecurity, and Industrial Control Systems and Operational Technology Cybersecurity), on the readiness of governmental institutions to counter cyber breaches in the ministries of the Eastern Region of the Kingdom of Saudi

Arabia. The study adopted the descriptive–analytical approach, employing a questionnaire as the main tool, distributed to a stratified random sample of (220) employees working in IT and cybersecurity departments. Data were analyzed using SPSS software. The results revealed a statistically significant positive impact at the ($\alpha \leq 0.05$) level of NCA standards on cybersecurity readiness, with the five dimensions collectively explaining (78.0%) of the variance in the dependent variable. Cybersecurity Governance emerged as the most influential dimension, followed by Cybersecurity Defense, Cybersecurity Resilience, Third–Party and Cloud Computing Cybersecurity, and lastly Operational Technology Cybersecurity. The study recommended accelerating policy review cycles, adopting the Zero Trust Architecture, conducting periodic cyber simulation drills, enhancing monitoring of cloud service providers, developing specialized cadres in OT security, and establishing a unified national platform for cyber threat intelligence sharing among governmental entities.

Keywords: Cybersecurity, National Cybersecurity Authority (NCA), Cyber Readiness, Cyber Breaches, Governmental Institutions, Eastern Region, Kingdom of Saudi Arabia.

ملحق (١): الاستبانة

السلام عليكم ورحمة الله وبركاته،،

يقوم الباحث بإجراء دراسة علمية بعنوان " أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات - دراسة ميدانية على وزارات المنطقة الشرقية"، وذلك استكمالاً لمتطلبات الحصول على الدرجة العلمية.

ونظراً لما تتمتعون به من خبرة ودراية في مجال تقنية المعلومات والأمن السيبراني، يتشرف الباحث بأن يضع بين أيديكم هذه الاستبانة، راجياً التكرم بقراءة فقراتها بدقة، والإجابة عنها بموضوعية، باختيار الإجابة التي تُعبّر عن وجهة نظركم. وتفضلوا بقبول تأكيد الباحث بأن جميع المعلومات الواردة ستُعامل بسرية تامة، ولن تُستخدم إلا لأغراض البحث العلمي فقط.

شاكراً لكم حسن تعاونكم،، الباحث

القسم الأول: البيانات الديموغرافية

١. الجنس: () ذكر () أنثى
٢. العمر: () أقل من ٣٠ () ٣٠ - أقل من ٤٠ () ٤٠ - أقل من ٥٠ () ٥٠ فأكثر
٣. المؤهل العلمي: () دبلوم () بكالوريوس () ماجستير () دكتوراه
٤. سنوات الخبرة في مجال تقنية المعلومات / الأمن السيبراني: () أقل من ٥ () ٥ - أقل من ١٠ () ١٠ - أقل من ١٥ () ١٥ فأكثر
٥. المسمى الوظيفي: () مدير إدارة () رئيس قسم () أخصائي/محلل () أخرى
٦. هل حصلت على شهادات مهنية في الأمن السيبراني (CISSP, CISA, ISO 27001 ...) ؟ () نعم () لا

القسم الثاني: فقرات الاستبانة

أولاً: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

البُعد الأول: حوكمة الأمن السيبراني

م	الفقرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تمتلك وزارتي استراتيجية معتمدة للأمن السيبراني متوافقة مع متطلبات NCA.					
2	تُحدّد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بوضوح داخل الهيكل التنظيمي للوزارة.					
3	تُراجع سياسات الأمن السيبراني وتُحدّث بشكل دوري وفق المستجدات التنظيمية.					
4	توفّر الإدارة العليا الدعم المالي والإداري اللازم لتطبيق ضوابط الأمن السيبراني.					

البُعد الثاني: تعزيز الأمن السيبراني

م	الفقرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5	تُطبّق في وزارتي إجراءات صارمة لإدارة الهويات والصلاحيات للوصول إلى الأنظمة.					
6	تُستخدم أنظمة متقدمة لحماية الشبكات وكشف التهديدات السيبرانية.					

					7 تُجرى عمليات دورية لإدارة الثغرات الأمنية واختبار الاختراق في وزارتي.
					8 تُطبّق ضوابط حماية البيانات والتشفير على الأصول المعلوماتية الحساسة.

البُعد الثالث: صمود الأمن السيبراني

م	الفقرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
9	تمتلك وزارتي خطة معتمدة لاستمرارية الأعمال تشمل جوانب الأمن السيبراني.					
10	تُجرى اختبارات دورية لخطط التعافي من الكوارث السيبرانية.					
11	تُحدَّث إجراءات النسخ الاحتياطي للبيانات الحيوية بشكل منتظم.					
12	تتوفر لدى وزارتي قدرات فعّالة للاستجابة السريعة للحوادث السيبرانية.					

البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

م	الفقرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
13	تتضمّن العقود مع مزوّدي الخدمات اشتراطات واضحة للأمن السيبراني.					

					14	تُقيّم المخاطر السيبرانية المتعلقة بالأطراف الخارجية بصورة منتظمة.
					15	تُطبّق ضوابط NCA الخاصة بأمن الحوسبة السحابية على الخدمات المستضافة.
					16	تُراقب أنشطة مزودي الخدمات السحابية للتحقق من التزامهم بمتطلبات الأمن.

البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية

م	الفقرة	موافق بشدة	موافق بشدة	محايد	غير موافق	غير موافق بشدة
17	تُطبّق في وزارتي ضوابط متخصصة لحماية أنظمة التقنية التشغيلية. (OT)					
18	تُفصل شبكات التقنية التشغيلية عن شبكات تقنية المعلومات بشكل آمن.					
19	تُجرى عمليات رصد مستمرة للأنشطة غير المعتادة في أنظمة التحكم.					
20	يُدرّب العاملون على الأنظمة التشغيلية على متطلبات الأمن السيبراني.					

ثانياً: الجاهزية للتصدي للاختراقات

م	الفقرة	موافق بشدة	موافق بشدة	محايد بشدة	غير موافق بشدة
1	تمتلك وزارتي قدرات وقائية فعالة تحول دون وقوع الاختراقات السيبرانية.				
2	تتوفر أدوات متقدمة لاكتشاف الهجمات السيبرانية في مراحلها الأولى.				
3	يستجيب فريق الأمن السيبراني لدينا للحوادث في زمن قياسي.				
4	تمتلك وزارتي خطة واضحة ومُختبَرة للتعافي من الحوادث السيبرانية.				
5	يتمتع الكادر التقني بالكفاءة اللازمة للتعامل مع التهديدات السيبرانية المتقدمة.				
6	تُجرى تمارين محاكاة دورية لاختبار جاهزية الوزارة للهجمات السيبرانية.				
7	تُوثَّق الحوادث السيبرانية ويُستفاد من دروسها في تحسين الجاهزية.				
8	تُتاح آليات واضحة للتواصل والتنسيق مع الجهات الوطنية عند وقوع الحوادث.				
9	يملك العاملون وعياً سيبرانياً يُمكنهم من التعرف على محاولات الاختراق.				

					10	تتوفر تقنيات حديثة لرصد التهديدات المتطورة (APT) داخل البيئة التقنية.
					11	تُراجع مؤشرات الأداء الخاصة بالجاهزية السيبرانية بصورة دورية.
					12	تستطيع وزارتي استئناف خدماتها الرقمية بسرعة بعد أي حادث سيبراني.

شاكرين لكم حسن تعاونكم

٣,٢. الخاتمة

٤. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

٤,١ . المقدمة

٤,٢ . توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

٤,٣ . اختبارات الصدق والثبات للاستبيانات

٤,٤. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)

٤,٥. اختبار الفرضيات ومناقشة النتائج

٤,٦. الخاتمة

٥. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

٥,١. حدود الدراسة والدراسات المستقبلية:

٥,٢. توصيات الدراسة:

٥,٣. الخاتمة:

قائمة المراجع

