

تقييم فاعلية ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات
المرضى واستمرارية الخدمات الصحية
دراسة ميدانية في تجمع نجران الصحي

إعداد الطالب

شذى ناصر اللافى

إشراف

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي

2025

Mid-Ocean University

College of Management

Master of Risk Management



**Evaluation of the Effectiveness of Cybersecurity Risk Management Practices
in Protecting Patient Data and Ensuring the Continuity of Health Services**

A Field Study in Najran Health Cluster.

Prepared by:

Shatha Nasser Allafi

Advisor:

Dr. Al-Faisal Abdul Hamid.

Dr. Fayez Jarad

Academic Year

2025

شكر وتقدير

﴿وَأَخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ﴾

لقد كانت الرحلة طويلة وصعبة،

لكنني أنجزتها، بفضل الله الذي سهل البدايات ومنحنا النهايات بفضلته وكرمه.

إلى من زين اسمي بأجمل الألقاب، ودعمني بلا شروط ومنحني بلا حدود، داعمي الأول في رحلتي، وعكازي، وقوتي، بعد الله. — إلى مصدر فخري وسروري: والدي العزيز.

إلى من جعل الله الجنة تحت قدميها، ومن احتضن قلبي قبل يديها، والتي خفت عني صعوباتي بدعواتها. إلى الامراة العظيمة، إلى معلمتي الأولى، التي غرزت في حب التميز والنجاح والمثابرة. — إلى أمي العظيمة.

إلى دعمي الثابت وأمان أيامي، إلى من شدّ أزرني فأصبحوا مصدر قوتي. إلى أفضل أيام حياتي وراحتهم، إلى قرة عيني. — إلى إخوتي وأخواتي الأعزاء.

إلى المعلمين الملهمين، الدكتور: فيصل عبد الحميد و الدكتور: فايز جراد شكراً لكل ما قدمتموه والذي ساهم في إثراء بحثي.

أهدي لكم هذا الإنجاز بفضل الله العظيم

الحمد لله على ما أنعم به علي، وأرجو أن يعينني ويجعلني مباركاً أينما كنت.

أخيراً:

تذكروا أن كل الاحلام تتحقق يا أصدقاء، وأن الأحلام التي لم تتحقق تنازل عنها أصحابها، وتكاسلوا عن السعي لها، وسقطوا من أول عثرة ولم ويعاودوا الوقوف!

وتذكروا أيضاً، أنكم لم تخلقوا عبثاً، ما ولدتموا كي تموتوا سدىً

لا خيب الله مساعيكم في مناكب الحياة، ولا أضاع لكم جهداً أو حلاًماً.

فلكم حق التمني، وهمة السعي، وحسن الظن والله سر التوقيت، وسر الإجابة، وسر الدهشة

جدول المحتويات

3	شكر وتقدير.....
8	فهرس الأشكال.....
9	فهرس الجداول.....
11	الفصل الأول: مقدمة.....
12	مقدمة
14	مشكلة الدراسة.....
16	أهمية الدراسة.....
18	أهداف الدراسة.....
19	تساؤلات الدراسة.....
20	فروض الدراسة.....
21	النظرية العلمية المتبعة لإعداد البحث.....
23	الفصل الثاني: الدراسات السابقة.....
24	مقدمة
24	متغيرات البحث.....
24	المتغير المستقل - إدارة مخاطر الأمن السيبراني.....
24	المتغير التابع - حماية بيانات المرضى.....
25	المتغير التابع - استمرارية الخدمات الصحية.....
26	مراجعة الدراسات السابقة.....
31	تحليل الدراسات السابقة.....
35	الإطار النظري للدراسة.....
37	الفصل الثالث: منهجية الدراسة.....
38	مقدمة
38	تصميم البحث.....

39	النموذج المفاهيمي للبحث
41	المنهج البحثي
41	نوع البحث
42	استراتيجية البحث
42	مجتمع الدراسة
42	المجتمع المستهدف
42	المجتمع المتاح
43	خصائص العينة
43	أسلوب المعاينة
44	تحديد حجم العينة
44	توزيع العينة
45	معدل الاستجابة المتوقع
45	إجراءات جمع البيانات
45	أداة جمع البيانات
46	صدق الأداة
47	ثبات الأداة
48	خطوات جمع البيانات
49	الاعتبارات الأخلاقية
50	حدود الدراسة
52	أساليب التحليل الإحصائي
52	معالجة البيانات
52	تنظيف وترميز البيانات
52	إدخال البيانات
52	التحليل الإحصائي الوصفي

53	التحليل الإحصائي الاستدلالي
54	أداة التحليل الإحصائي
55	الفصل الرابع: الدراسة الميدانية
56	مقدمة
57	التحليل الديموغرافي للعينة
57	الجنس (Gender)
58	العمر (Age)
59	المستوى التعليمي (Education)
59	الوظيفة الحالية (Job)
60	سنوات الخبرة (Experience)
61	التدريب على الأمن السيبراني (Training)
62	التحليل الوصفي لمحاور الدراسة
62	المحور الأول: تحديد المخاطر (Risk Identification - RI)
63	المحور الثاني: تقييم المخاطر (Risk Assessment - RA)
64	المحور الثالث: معالجة المخاطر (Risk Treatment - RT)
65	المحور الرابع: الرقابة على المخاطر (Monitoring Risks - MR)
65	حماية بيانات المرضى (Patient Data Protection - PDP)
67	استمرارية الخدمات الصحية (Service Continuity - SC)
68	التحديات التنظيمية والبشرية (Organizational & Human Challenges – CH)
70	ملخص المتوسطات الحسابية لجميع محاور الاستبانة
72	اختبار الفرضيات
72	اختبار الفرضية الأولى H1
75	اختبار الفرضية الثانية H2
76	اختبار الفرضية الثالثة H3

أثر الخصائص الديموغرافية على تقييم فعالية ممارسات إدارة المخاطر السيبرانية.....	80
التحليل التكاملي ومناقشة النتائج.....	84
التوصيات.....	88
التوصيات الإدارية والتنظيمية.....	88
التوصيات البحثية.....	92
المراجع.....	97
المراجع العربية.....	97
المراجع الأجنبية.....	97
الملاحق.....	101
ملحق (1): الاستبانة النهائية للدراسة.....	102
المستخلص.....	107
Abstract.....	108

فهرس الأشكال

- شكل 1: مخطط مراحل تصميم البحث 39
- شكل 2: النموذج المفاهيمي للبحث..... 40
- شكل 3: توزيع العينة حسب الجنس..... 57
- شكل 4: التوزيع النسبي للعينة حسب المستوى التعليمي..... 59
- شكل 5: نسبة المستجيبين الذين تلقوا تدريباً على الأمن السيبراني..... 61

فهرس الجداول

جدول 1: جدول مقارنة - أبرز نتائج الدراسات السابقة.....	31
جدول 2: نتائج اختبار كرونباخ ألفا للاختبار الاستطلاعي.....	47
جدول 3: معاملات ألفا كرونباخ لمحاول الاستبانة.....	56
جدول 4: التوزيع التكراري للينة حسب الفئات العمرية.....	58
جدول 5: توزيع الينة حسب الوظيفة الحالية.....	59
جدول 6: التوزيع التكراري للينة حسب فئات الخبرة.....	60
جدول 7: الإحصاءات الوصفية لمحور تحديد المخاطر.....	62
جدول 8: الإحصاءات الوصفية لمحور تقييم المخاطر.....	63
جدول 9: الإحصاءات الوصفية لمحور معالجة المخاطر.....	64
جدول 10: الإحصاءات الوصفية لمحور الرقابة على المخاطر.....	65
جدول 11: الإحصاءات الوصفية لمحور حماية بيانات المرضى.....	66
جدول 12: الإحصاءات الوصفية لمحور استمرارية الخدمات الصحية.....	67
جدول 13: الإحصاءات الوصفية لمحور التحديات التنظيمية والبشرية.....	68
جدول 14: الإحصاءات الوصفية لمحور الرضا عن الممارسات.....	69
جدول 15: ملخص المتوسطات الحسابية لجميع محاور الاستبانة.....	71
جدول 16: معامل ارتباط بيرسون بين ممارسات إدارة المخاطر وحماية بيانات المرضى.....	72
جدول 17: نتائج تحليل الانحدار الخطي البسيط (المتغير التابع: حماية بيانات المرضى).....	72
جدول 18: معاملات الانحدار.....	73
جدول 19: معاملات الارتباط بين أبعاد إدارة المخاطر وحماية بيانات المرضى.....	73
جدول 20: نتائج تحليل الانحدار المتعدد (المتغير التابع: حماية بيانات المرضى).....	74
جدول 21: معامل ارتباط بيرسون بين ممارسات إدارة المخاطر واستمرارية الخدمات.....	75
جدول 22: نتائج تحليل الانحدار الخطي البسيط (المتغير التابع: استمرارية الخدمات).....	75
جدول 23: معاملات الانحدار.....	75
جدول 24: معامل ارتباط بيرسون بين التحديات التنظيمية والبشرية وفعالية إدارة المخاطر.....	77
جدول 25: تحليل تفصيلي لمؤشرات التحديات وعلاقتها بفعالية إدارة المخاطر.....	77
جدول 26: اختبار t للفروق في فعالية إدارة المخاطر حسب مستوى التحديات.....	77
جدول 27: نتائج تحليل الانحدار المتعدد (المتغير التابع: فعالية إدارة المخاطر).....	78

جدول 28: اختبار t للفروق حسب الجنس.....	80
جدول 29: تحليل التباين الأحادي للفروق حسب المستوى التعليمي.....	80
جدول 30: اختبار Scheffe للمقارنات البعدية.....	81
جدول 31: تحليل التباين الأحادي للفروق حسب سنوات الخبرة.....	82
جدول 32: تحليل التباين الأحادي للفروق حسب الوظيفة.....	82
جدول 33: اختبار t للفروق حسب التدريب.....	83

الفصل الأول: مقدمة

مقدمة

تشهد مؤسسات الرعاية الصحية عالمياً تزايداً مطّرداً في الهجمات السيبرانية خلال السنوات الأخيرة. يُعزى ذلك إلى القيمة العالية للبيانات الصحية، إذ تعتبر بيانات المرضى البيانات الأكثر قيمة في السوق السوداء مقارنة بأي نوع آخر من البيانات (Clarke & Martin, 2023)، مما يجعلها هدفاً جذاباً. وقد أصبحت الرعاية الصحية أحد أكثر القطاعات استهدافاً بالهجمات الرقمية، مدفوعةً بانتشار السجلات الصحية الإلكترونية والأجهزة الطبية الموزعة (إنترنت الأشياء) دون أن يصاحب ذلك تعزيز مماثل في موارد الأمن السيبراني (Aldosari, 2025). ونتيجةً لهذه الهجمات، تعرّضت خصوصية المرضى وسرية معلوماتهم للخطر، وتضررت استمرارية الخدمات الصحية بشكل ملحوظ، حيث سجلت حالات ألغيت فيها إجراءات طبية واضطرت مستشفيات إلى تغيير مسار علاجي لمرضى بسبب اختراقات سيبرانية (Conduah et al., 2025). وتؤكد الإحصاءات الحديثة خطورة الوضع، فقد كان عام 2023 الأسوأ على الإطلاق من حيث خروقات البيانات الصحية في الولايات المتحدة، بواقع 725 خرقاً أمنياً كشف خلالها عن أكثر من 133 مليون سجل طبي (Alder, 2025). كما أن غالبية هذه الخروقات (نحو 80%) نتجت عن هجمات قرصنة أو برمجيات الفدية (Definitive Healthcare, 2024). ولا تقتصر تداعيات الهجمات على تسريب المعلومات فحسب، بل قد تؤدي أيضاً إلى تعطل الأنظمة الصحية وتأخير الرعاية مما يهدد سلامة المرضى بشكل مباشر (Clarke & Martin, 2023).

على الصعيد المحلي، تواجه المملكة العربية السعودية التحديات ذاتها في ظل التحول الرقمي السريع لقطاع الصحة ضمن رؤية 2030. فقد أظهرت تقارير حديثة أن المملكة رصدت حوالي 110 مليون تهديد سيبراني خلال عام 2022 في مختلف القطاعات (Saudi Healthcare Consulting, 2024)، كان القطاع الصحي من أبرزها تأثراً نظراً لحساسية بيانات المرضى وأهمية استمرارية الرعاية. وتتوافق هذه المعطيات مع حقيقة أن البيانات الصحية قد تفوق قيمتها المالية عشرات الأضعاف مقارنةً ببيانات مالية كبيانات البطاقات الائتمانية (Clarke & Martin, 2023)، مما يجعل حماية بيانات المرضى أولوية قصوى. ومن جهة أخرى، فإن استمرارية الخدمات الصحية أصبحت مرهونة بقدرة المنشآت على الصمود أمام الهجمات السيبرانية، إذ يمكن لهجوم واحد أن يشل مستشفى بأكمله ويوقف خدماته الحرجة مؤقتاً (الشهري & سلمان, 2024). هنا برزت أهمية تبني ممارسات فعّالة في إدارة مخاطر الأمن السيبراني لحماية سرية معلومات المرضى وضمان جاهزية الأنظمة واستمرارها في تقديم الخدمات دون انقطاع.

فإدارة مخاطر الأمن السيبراني هي عملية منهجية تهدف إلى تحديد التهديدات السيبرانية التي تواجه البنى التحتية للمعلومات الصحية، وتقييم مستويات الخطورة، ثم اعتماد الضوابط والإجراءات الكفيلة بتخفيف تلك المخاطر إلى مستويات مقبولة (Argaw et al., 2020). وتشمل هذه الممارسات وضع سياسات أمنية صارمة، وتطبيق معايير وأطر عمل معتمدة (مثل إطار الأمن السيبراني الصادر عن المعهد الوطني

للمعايير والتقنية (NIST)، إضافة إلى تدريب الكوادر ورفع الوعي الأمني، واستثمار تقنيات الحماية الحديثة لرصد الحوادث والاستجابة لها بكفاءة.

وبالرغم من الجهود المبذولة عالمياً ومحلياً، تشير الدلائل إلى وجود فجوة بين تزايد التهديدات وبين فعالية التدابير الأمنية الحالية في القطاع الصحي. فعلى سبيل المثال، أظهر مسح أجرته منظمة HIMSS عام 2021 أن معظم مؤسسات الرعاية الصحية تخصص 6% أو أقل فقط من ميزانية تقنية المعلومات للأمن السيبراني (HIMSS, 2024)، ولم تتغير هذه النسبة تقريباً على مدار أربع سنوات، مما يعكس نقص الاستثمار في حماية المعلومات الحيوية. كما أفاد 84% من المستشفيات في مسح HIMSS عام 2021 بأن العثور على مختصي أمن سيبراني مؤهلين وتوظيفهم يشكل تحدياً كبيراً، وأن 66% منها تواجه صعوبة في الاحتفاظ بالخبرات الأمنية بعد توظيفها (المرداس, 2023). هذه المعطيات تكشف أن العديد من المنشآت لا تزال عرضة للمخاطر بسبب محدودية الموارد البشرية والمالية المخصصة للأمن، أو بسبب قصور سياسات الحماية والتدريب. ومن هنا نميز مشكلة البحث الحالية، حيث من الضروري تقييم فاعلية ممارسات إدارة مخاطر الأمن السيبراني المطبقة حالياً في القطاع الصحي وقدرتها على تحقيق الغايتين الأساسيتين: حماية بيانات المرضى وضمان استمرارية الخدمات الصحية. يقدم هذا البحث دراسة ميدانية في تجمع نجران الصحي (أحد التجمعات الصحية الإقليمية في السعودية) للتحقق من مدى كفاءة ونجاعة هذه الممارسات في البيئة المحلية، وتتمثل الإضافة العلمية المتوقعة في تحديد جوانب القوة والضعف في منظومة الأمن السيبراني الصحي على المستوى الميداني. وبذلك تسهم الدراسة الحالية في سد فجوة معرفية مهمة، من خلال تقديم أدلة علمية حديثة حول واقع إدارة مخاطر الأمن السيبراني في قطاع صحي سعودي، وما يرتبط بها من تأثيرات على سلامة البيانات واستمرارية الرعاية.

مشكلة الدراسة

يشهد القطاع الصحي في العصر الرقمي اعتماداً متزايداً على الأنظمة الإلكترونية لإدارة البيانات الطبية وتقديم الخدمات الصحية، مما يجعله عرضة لتهديدات الأمن السيبراني بشكل غير مسبوق. يمكن للهجمات السيبرانية أن تؤدي إلى سرقة معلومات المرضى الحساسة أو تعطيل العمليات السريرية، الأمر الذي يشكل خطراً على خصوصية المرضى واستمرارية الرعاية الصحية.

تكشف الإحصائيات العالمية الحديثة عن تصاعد مقلق في الهجمات السيبرانية المستهدفة للقطاع الصحي. فقد كشف تقرير IBM للأمن السيبراني لعام 2023 أن متوسط تكلفة خرق البيانات في قطاع الرعاية الصحية بلغ 10.93 مليون دولار أمريكي، وهو الأعلى مقارنة بجميع القطاعات الأخرى للعام الثالث عشر على التوالي (IBM, 2025).

كما أظهرت دراسة مؤسسة Ponemon Institute أن 89% من مؤسسات الرعاية الصحية تعرضت لخرق بيانات واحد على الأقل خلال العام الماضي، فيما تعرض 45% منها لخمس خروقات أو أكثر (الرحال، 2025). وعلى الصعيد المحلي، وفي استطلاع أجرته شركة Deloitte Middle East على 45 مؤسسة صحية سعودية، أفاد 68% من المشاركين بأنهم واجهوا محاولة اختراق إلكتروني واحدة على الأقل خلال العام 2021، بينما أقر 23% منهم بحدوث خرق فعلي أدى إلى تسريب بيانات أو تعطيل خدمات (Shadadi et al., 2025).

في هذا السياق المعقد، تتبلور مشكلة البحث الرئيسية في الحاجة الملحة لتقييم علمي شامل لمدى فعالية ممارسات إدارة مخاطر الأمن السيبراني المطبقة في المؤسسات الصحية السعودية - متمثلة في تجمع نجران الصحي - في تحقيق هدفين استراتيجيين: حماية بيانات المرضى من الاختراقات، وضمان استمرارية الخدمات الصحية دون انقطاع أثناء التعرض للتهديدات السيبرانية. ورغم توفر العديد من الأطر والمعايير العالمية لإدارة المخاطر السيبرانية (مثل NIST و ISO 27001)، إلا أن السؤال الجوهرى يبقى: "إلى أي مدى تُطبّق هذه الممارسات بفعالية في الواقع العملي؟ وهل تحقق الأهداف المرجوة منها؟" تتجلى خطورة وأهمية معالجة هذه المشكلة من خلال أربعة أبعاد حرجية:

أولاً: البعد الأمني والخصوصية

يمكن لأي اختراق لبيانات المرضى أن يؤدي إلى عواقب وخيمة متعددة. فالسجلات الطبية الإلكترونية تحتوي على معلومات شخصية حساسة يمكن استغلالها في سرقة الهوية الطبية، حيث وجدت دراسة أن 27% من ضحايا سرقة الهوية الطبية واجهوا صعوبات في الحصول على رعاية صحية صحيحة بسبب تلوث سجلاتهم. كما تُستخدم في الابتزاز والتشهير، والاحتيال المالي حيث بلغت خسائر الاحتيال في التأمين الصحي في الولايات المتحدة 68 مليار دولار سنوياً (NHCAA, 2022).

ثانياً: البعد التشغيلي واستمرارية الخدمات

تهدد الهجمات السيبرانية قدرة المؤسسات الصحية على تقديم خدماتها بشكل كارثي. فهجوم WannaCry عام 2017 على هيئة الخدمات الصحية البريطانية (NHS) أدى إلى تعطيل 80 مستشفى و595 عيادة، مما نتج عنه إلغاء 19,000 موعد طبي وتأجيل 139 عملية جراحية، بتكلفة إجمالية بلغت 92 مليون جنيه إسترليني (Ghafur et al., 2019).

وفي الولايات المتحدة، كشفت دراسة أن 64% من المؤسسات التي تعرضت لهجمات برمجيات فدية اضطرت لتأجيل إجراءات طبية، و59% منها شهدت زيادة في معدلات تحويل المرضى. الأخطر من ذلك، أن هجمات برمجيات الفدية على المستشفيات ارتبطت بزيادة بنسبة 4% في معدلات الوفيات بين المرضى الذين عولجوا خلال فترة الهجوم (Portela et al., 2023).

ثالثاً: البعد الاجتماعي والثقة العامة

يمتد تأثير الخروقات إلى ثقة المجتمع في النظام الصحي. أظهرت الدراسات أن 81% من البالغين يعبرون عن قلق بالغ حول استخدام بياناتهم الصحية، و64% لا يتقنون بقدرة المؤسسات على حمايتهم، وأن 38% ممن علموا بوقوع خرق أحجموا عن مشاركة معلومات صحية مهمة مع أطبائهم خوفاً من تسريبها، مما قد يؤدي إلى تشخيصات خاطئة (Grande et al., 2020).

في ضوء الأبعاد الحرجة المذكورة، تُثار التساؤلات التالية:

- ما هي ممارسات إدارة مخاطر الأمن السيبراني الحالية في تجمع نجران الصحي؟ تنبثق أهمية هذا التساؤل من ضرورة تحديد الإجراءات والخطط المطبقة فعلياً لحماية البيانات واستمرارية الخدمة، إذ لا يمكن تقييم الفاعلية دون فهم الوضع الراهن للممارسات المعمول بها. يشمل ذلك التعرف على سياسات الأمن الإلكتروني، وأنظمة الحماية التقنية والإدارية، ومدى تكامل الأمن السيبراني ضمن إطار إدارة المخاطر بالمؤسسة.

- ما مدى فعالية هذه الممارسات في حماية بيانات المرضى من الاختراقات والانتهاكات؟ ينبع هذا التساؤل من خطورة الانتهاكات السيبرانية على خصوصية المرضى وسلامتهم. فالهجمات الإلكترونية التي تستهدف السجلات الصحية قد تؤدي إلى كشف بيانات صحية حساسة، مما يعرض المؤسسات لعواقب قانونية وخسائر مالية وسمعة سلبية، مما يؤكد ضرورة تقييم ما إذا كانت الإجراءات الحالية كافية لمنع حدوث اختراقات مشابهة.

- ما مدى فعالية هذه الممارسات في ضمان استمرارية الخدمات الصحية أثناء التعرض للهجمات السيبرانية؟ يُطرح هذا السؤال نظراً لتأثير الهجمات الإلكترونية على توفر الخدمات الطبية. إن انقطاع الأنظمة الصحية نتيجة هجوم سيبراني قد يمنع الطواقم الطبية من الوصول إلى معلومات

المرضى أو استخدام الأجهزة الطبية الضرورية لرعايتهم. وقد شهدت مؤسسات صحية حالات تعطل للإسعاف والعمليات الجراحية أثناء الهجمات السيبرانية، مما يجعل تقييم خطط الطوارئ واستمرارية الأعمال جزءاً أساسياً من هذه الدراسة. لذا يتعين التحقق مما إذا كان لدى تجمع نجران الصحي خطط وتعزيزات كافية لضمان استمرار تقديم الرعاية حتى في أسوأ السيناريوهات.

• ما هي التحديات والثغرات الرئيسية في ممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي؟ يستند هذا التساؤل إلى ضرورة تحديد جوانب القصور - إن وجدت - في المنظومة الحالية. فقد تكون هناك تحديات تتعلق بضعف الوعي الأمني لدى العاملين أو نقص التدريب، مما قد يجعل العامل البشري نقطة ضعف بارزة. كما قد تواجه المؤسسة عقبات في تحديث البنية التحتية التقنية أو الامتثال للمعايير الدولية مثل معايير HIPAA الأمريكية و GDPR الأوروبية. إن الكشف عن هذه التحديات سيساعد في اقتراح توصيات عملية لتحسين مستوى الأمن السيبراني وضمان حماية أفضل لبيانات المرضى واستمرارية الخدمات.

تمثل هذه الأسئلة جوهر مشكلة البحث، وتسعى الدراسة للإجابة عنها من خلال التحليل الميداني الدقيق والتقصي العلمي المنهجي في بيئة تجمع نجران الصحي. فبينما تؤكد الإحصائيات خطورة التهديدات المتصاعدة - من حيث حجم الخروقات، والتكاليف المالية، والخسائر البشرية، والفجوة في الكوادر المتخصصة - تبقى الأدلة التجريبية حول فعالية الممارسات الأمنية المطبقة في البيئات الصحية السعودية محدودة للغاية. ومن هنا تبرز الحاجة الماسة لهذه الدراسة التقييمية الشاملة، التي لا تكتفي بوصف الممارسات الموجودة، بل تقيس فعاليتها الفعلية في حماية بيانات المرضى وضمان استمرارية الخدمات، وتحدد الثغرات والتحديات بدقة علمية. إن نتائج هذه الدراسة ستوفر أدلة علمية موثوقة تدعم صناع القرار في تجمع نجران الصحي خاصة، والقطاع الصحي السعودي عامة، في تطوير استراتيجيات أمنية أكثر فعالية، وتخصيص الموارد بكفاءة أعلى، وسد الفجوات الحرجة، وصولاً لتحقيق أهداف رؤية 2030 في بناء قطاع صحي رقمي آمن ومستدام يحمي خصوصية المواطنين ويضمن استمرارية الخدمات الحيوية في جميع الظروف، مما يسهم في تعزيز أمن المعلومات الصحية والموثوقية التشغيلية.

أهمية الدراسة

تأتي أهمية هذا البحث من جوانب عدة علمية وعملية تتقاطع مع أولويات مجال إدارة المخاطر والأمن السيبراني الصحي على المستويين العالمي والمحلي. من الناحية العلمية، تستجيب الدراسة لحاجة ملحة لسد الفراغ في الأدبيات حول فاعلية ضوابط الأمن السيبراني في بيئات الرعاية الصحية، خاصة في سياق الدول النامية ومنطقة الشرق الأوسط. معظم الدراسات السابقة تطرقت إلى أمن المعلومات الصحية من زوايا تقنية أو تنظيمية عامة، دون تقييم ميداني معمق لمدى نجاح ممارسات إدارة المخاطر في تحقيق أهدافها الأساسية (حماية البيانات واستمرارية الخدمة). على سبيل المثال، قدّمت دراسة (عفيفي، 2024) تحليلاً لتطبيق إدارة

المخاطر في مستشفيات جدة وخلصت إلى تحسّن ملموس في جودة الرعاية الصحية بنسبة 60% وفي سلامة المرضى بنسبة 50% بعد تطبيق نظم إدارة المخاطر. غير أن تلك الدراسة ركزت على إدارة المخاطر بشكل شمولي وتأثيره على الجودة والسلامة، ولم تفرد بحثاً تفصيلياً للجوانب السيبرانية البحتة أو لاستمرارية الخدمات خلال الحوادث الرقمية. هنا تبرز مساهمة الدراسة الحالية، إذ تتخصص في إدارة مخاطر الأمن السيبراني على وجه التحديد، وتركز على مخرجات نوعية (حماية البيانات، واستمرارية الخدمة) لم تُدرس بعمق كافٍ في البيئة البحثية العربية. وبالتالي، تضيف هذه الدراسة إلى رصيد المعرفة تصوراً أكثر دقة وتخصصاً لكيفية عمل الضوابط الأمنية السيبرانية في الواقع العملي، ومدى كفاءتها في التصدي للتهديدات الحالية.

علاوة على ذلك، نأمل من خلال الدراسة الحالية أن نُثري الأدبيات العالمية من خلال تقديم بيانات من سياق جديد (المملكة العربية السعودية)، وهو سياق ذو أهمية متزايدة في ظل التحول الرقمي الشامل الذي تشهده المملكة. فوفق رؤية السعودية 2030، يتم تحديث البنية التحتية الصحية رقمياً مع الالتزام بالمعايير الدولية للأمن السيبراني (Mani & Goniewicz, 2024)، وقد أنشأت المملكة هيئات مختصة مثل الهيئة الوطنية للأمن السيبراني (NCA) لوضع أطر تنظيمية لحماية البيانات الحساسة وتعزيز مرونة القطاعات الحيوية (Alharthi, 2021). وعلى الرغم من هذه الجهود، لا تزال البحوث الأكاديمية المتوفرة حول قياس نتائج تلك السياسات محدودة. من هنا، ستساهم هذه الدراسة في تقييم مخرجات الاستراتيجية الوطنية للأمن السيبراني في قطاع الصحة السعودي بشكل غير مباشر، عبر دراسة حالة تفصيلية في أحد التجمعات الصحية. إن نتائج هذه الدراسة الميدانية – سواءً أكدت فعالية الإجراءات الحالية أو أبرزت جوانب قصور – ستوفر مؤشرات علمية قيّمة لصنّاع القرار ولمسؤولي الأمن في القطاع الصحي حول ما تم إنجازه وما يلزم تحسينه. وبذلك، تتقاطع الأهمية العلمية مع الأهمية التطبيقية، حيث أن التوصيات المستندة إلى الأدلة التي ستخرج بها الدراسة يمكن أن تدعم جهود تطوير سياسات وإجراءات الأمن السيبراني على مستوى التجمعات الصحية والمستشفيات السعودية كافة.

ومن الزاوية التطبيقية، تأتي أهمية الدراسة في أنها تتعامل مع أمن معلومات المرضى الذي يُعدّ ركناً أساسياً في جودة الرعاية الصحية وثقة الجمهور في النظام الصحي. فأَي اختراق لبيانات المرضى لا يمثل مجرد خرق للخصوصية فحسب، بل قد يعرّض المرضى لمخاطر متعددة (كالتشهير أو الاحتيال المالي أو حتى الأخطاء الطبية الناتجة عن تغييرات غير مرخصة في السجلات). عليه، فإن حماية بيانات المرضى ليست ترفاً تقنياً بل ضرورة أخلاقية وقانونية لسلامة المرضى وحقوقهم. تؤكد منظمة الصحة العالمية (WHO) ذلك بتعريفها أمن المعلومات الصحية كإجراءات تضمن سرية معلومات المريض وسلامتها وتوفرها عند الحاجة (Conduah et al., 2025). وفي هذا السياق، يتفق الخبراء على أن نجاح مبادرات التحول الرقمي الصحي يعتمد بشكل كبير على مدى قوة الأمن السيبراني المصاحب لها (Hakami et al., 2024). لذا، فإن دراستنا – عبر تقييمها لفعالية الممارسات الأمنية – تقدم مقياساً عملياً لمدى جاهزية منظومة تجمع نجران

الصحي للتعامل مع المخاطر الرقمية دون تعطيل الخدمات. فإذا أثبتت الدراسة مثلاً وجود قصور في جانب معين (كالتدريب أو تقنية الحماية) يؤثر على استمرار الخدمة، فسيُمكن ذلك الجهات المعنية من اتخاذ إجراءات تصحيحية موجّهة وسريعة (مثل رفع ميزانية الأمن، أو إدخال تقنيات رصد جديدة، أو تكثيف التدريب للموظفين).

كما تُلقي الدراسة الضوء على التحديات الخاصة بالسياق السعودي في مجال الأمن السيبراني الصحي. فالمملكة تمتلك بعض الخصوصيات: كالنمو المتسارع للبنية التحتية الصحية الرقمية، والتنوع بين مستشفيات حكومية وخاصة ضمن تجمعات صحية، بالإضافة إلى البيئة التنظيمية المتطورة حديثاً في الأمن السيبراني. إن تحديد كيف تؤثر هذه العوامل على فعالية الأمن السيبراني (سلباً أو إيجاباً) سيساعد في تصميم استجابات مخصصة للسياق المحلي بدلاً من الاعتماد الكلي على توصيات عامة قد لا تراعي الفروق المحلية. على سبيل المثال، إذا كشفت الدراسة أن نقص الكفاءات الوطنية في الأمن السيبراني يشكل عائقاً بارزاً، فإن الحل قد يكمن في تعزيز الشراكات مع الجامعات وبرامج تأهيل الكوادر، أو زيادة الحوافز لاستقطاب الخبراء. أما إذا تبين أن بعض المستشفيات لا تطبق سوى الحد الأدنى من ضوابط الحماية الإلكترونية، فذلك قد يستدعي تشديد الرقابة والحوكمة أو إلزامية معايير أعلى من قبل الجهات التنظيمية.

يجدر بالذكر أن نتائج هذه الدراسة لن تفيد تجمع نجران الصحي وحده، بل تمتد أهميتها إلى مستوى التجمعات الصحية الأخرى والمستشفيات العامة في المملكة التي تشترك في خصائص مماثلة. حيث يمكن تعميم الدروس المستفادة والتوصيات على نطاق أوسع لتحسين جاهزية القطاع الصحي ككل ضد الأخطار السيبرانية. وفي المحصلة، يحقق هذا البحث أهمية متعددة المستويات: فهو يسد فجوة علمية في الأدبيات بإضافته معرفة نوعية عن الأمن السيبراني الصحي في المملكة، ويقدم أدوات تقييم عملي لصناع القرار ومديري المستشفيات حول فعالية ممارسات الحماية الحالية، كما يدعم التوجه الاستراتيجي الوطني نحو بناء قطاع صحي رقمي آمن ومتواصل الخدمات، مساهماً بذلك في رفع موثوقية النظام الصحي وحماية صحة المجتمع وحقوقه في العصر الرقمي.

أهداف الدراسة

انطلاقاً من أسئلة الدراسة وصياغة الفرضيات، تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف البحثية المحددة على النحو التالي:

1. تقييم فعالية ممارسات إدارة مخاطر الأمن السيبراني الحالية في حماية بيانات المرضى بتجمع نجران الصحي. يشمل ذلك قياس مستوى الحماية المتحقق للبيانات الحساسة (السجلات الطبية الإلكترونية وبيانات المرضى الشخصية) في ضوء الإجراءات والضوابط الأمنية المطبقة حالياً، وتحديد مدى كفايتها في منع الاختراقات والانتهاكات للخصوصية.

2. تقييم مدى إسهام ممارسات إدارة مخاطر الأمن السيبراني في ضمان استمرارية الخدمات الصحية في تجمع نجران الصحي. ويشمل ذلك تحليل قدرة هذه الممارسات على تقليل فترات توقف الأنظمة الصحية أثناء الحوادث الإلكترونية، ودورها في الاستجابة الفعالة للطوارئ التقنية بحيث لا تتعطل الخدمات العلاجية والتشخيصية الحيوية.

3. تحديد وتحليل التحديات والعوامل المؤثرة على فعالية إدارة مخاطر الأمن السيبراني في البيئة المدروسة. يتضمن هذا الهدف الكشف عن أبرز المعوقات (كالعجز في التمويل، نقص الكوادر المؤهلة، ضعف التدريب، مقاومة التغيير التقني، إلخ) التي قد تحد من نجاح برامج الأمن السيبراني، بالإضافة إلى تحليل تأثير كل من هذه العوامل على مستوى الأمان السيبراني واستمرارية العمل الصحي.

4. اقتراح توصيات واستراتيجيات تعزيزية مبنية على نتائج الدراسة، بهدف رفع كفاءة إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي. ستركز هذه التوصيات على معالجة نقاط الضعف المكتشفة وتعزيز نقاط القوة، بما في ذلك تحسين سياسات الأمن، وتطوير برامج تدريب ووعي أكثر فعالية، وتعزيز الدعم الإداري والموارد المخصصة للأمن السيبراني، بالإضافة إلى توظيف أحدث التقنيات والمعايير الدولية الملائمة للسياق السعودي.

من خلال تحقيق ما سبق، تطمح الدراسة إلى تقديم فهم شامل ومدعوم بالأدلة حول وضع الأمن السيبراني الصحي في التجمع محل الدراسة، وصياغة خارطة طريق عملية لتحسين إدارة المخاطر بما يتوافق مع أفضل الممارسات العالمية وخصوصية البيئة المحلية.

تساؤلات الدراسة

استناداً إلى مشكلة الدراسة، تم تحديد سؤال رئيسي تنبثق عنه عدة أسئلة فرعية تغطي مختلف جوانب الموضوع محل البحث. السؤال الرئيسي للدراسة هو:

إلى أي مدى تُسهّم ممارسات إدارة مخاطر الأمن السيبراني المطبقة في تجمع نجران الصحي في حماية بيانات المرضى وضمان استمرارية الخدمات الصحية؟

وينتفع عن هذا السؤال الرئيسي الأسئلة الفرعية التالية:

1. ما أبرز ممارسات إدارة مخاطر الأمن السيبراني المطبقة حالياً في تجمع نجران الصحي؟
2. ما مدى فعالية هذه الممارسات في حماية سرية وسلامة بيانات المرضى من الهجمات السيبرانية؟
3. كيف تساهم ممارسات إدارة المخاطر السيبرانية في ضمان استمرارية تقديم الخدمات الصحية دون انقطاع أثناء التعرض للتهديدات السيبرانية؟

4. ما التحديات الرئيسية التي تواجه تطبيق ممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي، وكيف تؤثر هذه التحديات على فعالية تلك الممارسات؟

تهدف هذه الأسئلة الفرعية إلى تفصيل أبعاد السؤال الرئيسي، بحيث يغطي كل سؤال جانباً محدداً يساهم في الإجابة الشاملة عن مدى فعالية ممارسات إدارة المخاطر السيبرانية في البيئة المستهدفة للدراسة.

فروض الدراسة

تطرح الدراسة الفرضيات التالية كإجابات متوقعة على أسئلة البحث:

1. الفرضية الأولى: توجد علاقة ذات دلالة إحصائية موجبة بين تطبيق ممارسات إدارة مخاطر الأمن

السيبراني وبين مستوى حماية بيانات المرضى في تجمع نجران الصحي. بمعنى آخر، يساهم التطبيق الفعال لمنهجيات إدارة المخاطر (مثل سياسات الأمن، وأنظمة الحماية التقنية، وإجراءات التحكم بالوصول) في تقليل حوادث اختراق البيانات وتسريبها، مما يؤدي إلى رفع مستوى سرية وسلامة معلومات المرضى.

2. الفرضية الثانية: توجد علاقة ذات دلالة إحصائية موجبة بين تطبيق ممارسات إدارة مخاطر

الأمن السيبراني وبين استمرارية الخدمات الصحية في تجمع نجران الصحي. أي أن التحسين في إدارة المخاطر السيبرانية يرتبط بانخفاض معدلات تعطل الأنظمة والخدمات الطبية، وبقدرة أعلى للمرافق الصحية على الصمود أمام الهجمات دون انقطاع كبير في الرعاية المقدمة.

3. الفرضية الثالثة: تؤثر التحديات التنظيمية والبشرية (مثل نقص الموارد المالية أو البشرية

المخصصة للأمن السيبراني، وضعف التدريب والوعي الأمني، ومقاومة التغيير التقني لدى الكوادر) بشكل سلبي معنوي على فعالية ممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي. وتعني هذه الفرضية أنه كلما ازدادت حدة هذه المعوقات، انخفض مستوى فاعلية برامج إدارة المخاطر السيبرانية وقدرتها على تحقيق أهدافها في الحماية والاستمرارية.

ستخضع هذه الفرضيات للاختبار والتحليل الإحصائي من خلال البيانات الميدانية، وذلك للتحقق من صحتها أو نفيها في سياق تجمع نجران الصحي. تجدر الإشارة إلى أن قبول أي من الفرضيات أعلاه يعني تأكيد وجود أثر أو علاقة ذات دلالة، في حين أن رفضها سيشير إلى غياب تأثير يُعتمد به إحصائياً.

النظرية العلمية المتبعة لإعداد البحث

تستند هذه الدراسة إلى نموذج نظري تكاملي يجمع بين ثلاثة أطر علمية معترف بها دولياً في مجالات الأمن السيبراني وإدارة المخاطر واستمرارية الأعمال، بهدف بناء أساس منهجي متين لتقييم فاعلية ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات المرضى وضمان استمرارية الخدمات الصحية. ويأتي هذا الدمج استجابةً للحاجة إلى إطار شامل يربط بين الأبعاد التقنية والتنظيمية والبشرية التي تؤثر في أمن المعلومات بالقطاع الصحي، خاصة في ظل ارتفاع حجم الهجمات السيبرانية على المؤسسات الصحية عالمياً بنسبة تتجاوز 74% خلال السنوات الثلاث الأخيرة (WHO, 2021; HIMSS, 2022).

يرتكز النموذج النظري أولاً على إطار الأمن السيبراني (NIST Cybersecurity Framework (CSF)، الذي يعدّ الأكثر استخداماً في القطاعات الحيوية. ويقوم هذا الإطار على خمس وظائف رئيسية: التعرف (Identify)، الحماية (Protect)، الكشف (Detect)، الاستجابة (Respond)، والتعافي (Recover) (NIST, 2020). تمثل هذه الوظائف سلسلة مترابطة من الأنشطة والسياسات والإجراءات الهادفة إلى تقليل احتماليات الاختراق وضمان استمرارية العمليات، وهو ما ينسجم مباشرةً مع أهداف الدراسة الحالية التي تسعى إلى تقييم تطبيق تلك الممارسات داخل تجمع نجران الصحي. وقد أكدت دراسات حديثة كدراسة Clarke & Martin (2023) أن تطبيق NIST-CSF في المستشفيات يسهم في تحسين مؤشرات الحماية بنسبة تتراوح بين 35%-50% مقارنة بالمؤسسات التي لا تعتمد إطاراً منهجياً لإدارة المخاطر.

ويرتكز النموذج النظري ثانياً على مبادئ إدارة المخاطر وفق معيار ISO 31000، الذي يؤكد على مراحل التعرف على المخاطر، تحليلها، تقييمها، ثم اتخاذ قرارات المعالجة المناسبة (ISO, 2018). وتعرّز هذه المنهجية قدرة الباحث على قياس فاعلية الضوابط الأمنية من خلال مؤشرات كمية تتعلق باحتمالية وقوع الحوادث، وشدتها، وقدرة المنظمة على الاستجابة والتعافي. وتشير الأدبيات الحديثة — مثل دراسة (Pool et al., 2024) — إلى أن المؤسسات الصحية التي تطبق إدارة مخاطر ممنهجة وفق ISO 31000 لديها قدرة أعلى على اتخاذ قرارات متوازنة بين الاستثمار في التقنيات والأطر التنظيمية.

أما الركيزة الثالثة للنموذج فهي مستمدة من إطار إدارة استمرارية الأعمال ISO 22301، الذي يؤكد على ضرورة امتلاك المنظمات الصحية لخطط استجابة واستعادة مؤسسية، بما في ذلك تحديد العمليات الحرجة، تحليل تأثير الكوارث، واختبار خطط الاستمرارية بشكل دوري (ISO, 2019). وقد بيّنت مراجعات حديثة (Kanaan et al., 2024) أن استمرارية الأعمال في القطاع الصحي ترتبط مباشرةً بمستوى النضج السيبراني للمؤسسة، وأن وجود خطة استمرارية أعمال فعّالة يحدّ من زمن التوقف التشغيلي بنسبة تصل إلى 60%.

ومن خلال دمج هذه الأطر الثلاثة NIST—، ISO 31000، —ISO 22301 تتطرق الدراسة من نموذج نظري مُحكم يربط بشكل ديناميكي بين:

1. ممارسات إدارة المخاطر السيبرانية (المتغير المستقل).

2. وحماية بيانات المرضى واستمرارية الخدمات الصحية (المتغير التابع)

3. العوامل التنظيمية والبشرية التي تؤثر في العلاقة بين المتغيرين.

ينسجم هذا التنبؤ للمدخل التكاملي مع التوجهات الحديثة في الأدبيات، التي تؤكد عدم كفاية الاعتماد على الضوابط التقنية وحدها دون تعزيز الجاهزية التنظيمية والبشرية، خصوصاً في المؤسسات الصحية الأكثر عرضة للهجمات (Rizzoni et al., 2022).

الفصل الثاني: الدراسات السابقة

مقدمة

تشكّل الدراسات السابقة أساساً جوهرياً لأي بحث أكاديمي، إذ تساهم في بناء الإطار النظري للموضوع وتحديد الفجوات البحثية المرتبطة به، مما يساعد على صياغة سؤال البحث وتوجيه منهجية الدراسة. في سياق إدارة مخاطر الأمن السيبراني بالقطاع الصحي، فإن مراجعة الأدبيات العلمية تُبرز ما توصلت إليه الأبحاث حول حماية بيانات المرضى واستمرارية الخدمات الصحية، كما تكشف عن الثغرات التي لم تُعالج بعد في المعرفة الحالية. وبذلك، يربط هذا القسم بين ما هو معروف علمياً وبين إشكالية الدراسة الراهنة، مما يُبرز مبررات الحاجة إلى البحث الحالي.

متغيرات البحث

المتغير المستقل - إدارة مخاطر الأمن السيبراني

يشير هذا المفهوم إلى منهجية منظمة لتحديد التهديدات السيبرانية التي تواجه المؤسسات الصحية وتقييمها ومعالجتها بشكل منهجي. تشمل ممارسات إدارة المخاطر السيبرانية وضع سياسات وإجراءات أمنية تعتمد معايير معيارية (مثل أطر NIST و ISO 27001) وتطبيق ضوابط تقنية وإدارية تهدف لتقليل احتمالية وقوع الحوادث السيبرانية أو تخفيف أضرارها. تؤكد الدراسات أن تبني إطار حوكمة أمنية موحد في المؤسسات الصحية يعزز قدرتها على إدارة المخاطر بشكل فعال (Božić, 2024)، ويوفر نهجاً منظماً لتحسين الوضع الأمني العام. كما تشدّد الأدبيات على أن الإدارة الفعالة لمخاطر الأمن السيبراني تتطلب تكاملاً بين الالتزام بالمعايير التنظيمية وإجراءات التقييم المنتظم للمخاطر والتدريب المستمر والتقنيات المتقدمة وخطط الاستجابة للحوادث (Božić, 2024)، مما يبرز الطبيعة المتعددة الأبعاد لهذا المتغير.

المتغير التابع - حماية بيانات المرضى

يُقصد بها الحفاظ على سرية وسلامة وتوفير المعلومات الصحية الشخصية (مثل السجلات الطبية الإلكترونية) ومنع الوصول غير المصرح لها أو الإفصاح غير القانوني عنها. تواجه المنظمات الصحية تحديات متزايدة في هذا الجانب نظراً لتصادم وتيرة الهجمات الإلكترونية التي تستهدف البيانات الطبية القيّمة. فقد بينت إحدى الدراسات التحليلية أن الحوادث الاختراقية (القرصنة/هجمات تقنية المعلومات) هي السبب الأبرز لغالبية خروقات بيانات الرعاية الصحية، تليها التسريبات الداخلية غير المصرح بها (Seh et al., 2020)، مما يدل على ارتفاع مستوى التهديد الخارجي والداخلي لخصوصية المرضى. وقد نجم عن ذلك ازدياد مطّرد في وتيرة الخروقات وحجم البيانات المكشوفة وتكاليفها على المؤسسات الصحية. بناءً عليه، توصي البحوث بضرورة تبني بروتوكولات أمنية صارمة لحماية بيانات المرضى، بما في ذلك تقنيات التشفير وأنظمة التحكم بالوصول وآليات التدقيق الدوري على استخدام البيانات الحساسة. فمثلاً أكّدت الدراسات أن اختراق السجلات الصحية الإلكترونية قد يؤدي إلى سرقة الهوية وخسائر مالية وتدهور ثقة

المرضى، ودعوا إلى تشديد سياسات حماية البيانات واعتماد بروتوكولات أمنية متقدمة (مثل التشفير وتقييد صلاحيات الوصول) للحد من تلك الخروقات (Božić, 2024). إذا يُعتبر متغير حماية بيانات المرضى مؤشراً أساسياً لفعالية ممارسات الأمن السيبراني في المؤسسات الصحية.

المتغير التابع - استمرارية الخدمات الصحية

تعني قدرة المنشآت الصحية على مواصلة تقديم خدمات الرعاية والعمليات التشغيلية بشكل طبيعي دون انقطاع أو توقف ملحوظ حتى في حال حدوث أحداث طارئة أو هجمات سيبرانية. أصبح ضمان الاستمرارية تحدياً استراتيجياً في ظل الاعتماد الكبير على الأنظمة الرقمية في المستشفيات، فالهجمات السيبرانية قد تؤدي إلى شلل أنظمة المستشفى وإعاقة الرعاية الصحية، مما يعرّض سلامة المرضى للخطر المباشر. على سبيل المثال، أظهر تحليل لأحد الهجمات الشهيرة (هجوم برنامج الفدية WannaCry عام 2017) أن المستشفيات التي تأثرت بالهجوم شهدت انخفاضاً يبلغ حوالي 6% في عدد الحالات المقبولة يومياً -بما في ذلك تراجع 4% في حالات الطوارئ - أثناء فترة الهجوم مقارنة بالمستشفيات غير المتأثرة (Ghafur et al., 2019). هذه المؤشرات تدل على التأثير الخطير للهجمات السيبرانية على استمرارية خدمات الرعاية. لذلك، يتطلب الحفاظ على استمرارية الخدمات تبني خطط واستراتيجيات شاملة للتعامل مع الأزمات السيبرانية، مثل وجود خطط طوارئ واستعادة للأنظمة ونسخ احتياطية للبيانات وتمارين استجابة منتظمة. وتنبّه الدراسات الحديثة إلى ضرورة دمج إدارة مخاطر الأمن السيبراني ضمن إطار إدارة استمرارية الأعمال في القطاع الصحي، حيث تبين أن النضج في ممارسات إدارة المخاطر الأمنية يرتبط إيجابياً بفعالية خطط استمرارية الخدمة وقدرة المنشأة الصحية على الصمود أمام الهجمات. أي أن وجود هيكلية قوية لإدارة المخاطر (بما في ذلك تقييم المخاطر ومعالجتها بشكل دوري) من شأنه ترجمة الاستثمارات الأمنية إلى مرونة تشغيلية أكبر في وجه الحوادث (Kanaan et al., 2024).

مراجعة الدراسات السابقة

بدأ الاهتمام الأكاديمي بقضية أمن المعلومات الصحية يتصاعد مع تكرار حوادث اختراق البيانات الصحية عالمياً. فقد أُجريت دراسة مراجعة شاملة لتحليل أوجه القصور والفشل في حماية البيانات الصحية الشخصية عبر مختلف المؤسسات الصحية. شملت هذه الدراسة (Pool et al., 2024) تحليلاً منهجياً لحالات اختراق البيانات وتقارير الثغرات الأمنية بهدف استنباط أنماط مشتركة وأسباب جذرية لتلك الإخفاقات. وقد كشفت نتائج المراجعة أن الجهات الخارجية الخبيثة هي غالباً المصدر الأساسي لانتهاكات بيانات المرضى، حيث يستغل المهاجمون نقاط الضعف في أنظمة السجلات الصحية الإلكترونية للتسلل إلى قواعد البيانات وسرقة المعلومات. وأبرزت الدراسة أن هذه الخروقات تُعزى في كثير من الأحيان إلى ثغرات تقنية وإجرائية مثل ضعف بروتوكولات المصادقة وعدم كفاية التشفير أو غياب أنظمة التتبع والتدقيق. لذا شدد الباحثون على ضرورة تعزيز الضوابط التقنية كالتشفير القوي والتحكم الصارم في صلاحيات الوصول للبيانات، بالإضافة إلى آليات مراقبة وتدقيق منتظمة لاكتشاف أي نشاط غير طبيعي في نظم المعلومات الصحية. امتازت هذه الدراسة بسعتها وشمولها للمؤشرات عبر نطاق واسع من البيئات الصحية، ما وقرّ نموذجاً عاماً للمخاطر يمكن أن تستفيد منه المؤسسات لتحسين ممارساتها. ومع ذلك، يُؤخذ على الدراسة اعتمادها على بيانات ثانوية منشورة سلفاً (تقارير حوادث وبيانات أرشيفية) مما قد يترك بعض التفاصيل النوعية غير مكتشفة، كما أنها لم تختبر فعلياً فاعلية التدابير المقترحة بل اكتفت بتوصيات عامة تستند للاستدلال من الحالات السابقة.

وفي سياق مماثل، قدّمت الدراسة (Božić, 2024) استعراضاً واسعاً لحوكمة الأمن السيبراني في الرعاية الصحية، ركّزت فيه على استعراض السياسات والمعايير والممارسات الراهنة والتحديات التي تواجه تحسين الوضع الأمني. تعد دراسة بوزيتش بمثابة مراجعة أدبيات نقدية جمعت بين مصادر أكاديمية وصناعية وتنظيمية لرسم صورة شاملة عن المشهد الحالي. أشار الباحث إلى أن القطاع الصحي يتعرض بشكل متزايد لهجمات سيبرانية متطورة (مثل برامج الفدية والتصيد الاحتيالي والتهديدات الداخلية) في ظل التوسع في التقنيات الحديثة كإنترنت الأشياء الطبية والطبّ عن بُعد. كما نوّه إلى تحديات نقص الموارد في المؤسسات الصحية الأصغر، سواء من حيث التمويل أو ندرة الكوادر المتخصصة بالأمن السيبراني، مما يعيق تطبيق إجراءات حماية كافية. أبرزت الدراسة أيضاً تعقيد البنية التحتية الصحية وتعدد الأنظمة والأجهزة المتصلة (بما في ذلك أجهزة الجهات الخارجية)، ما يخلق نقاط دخول كثيرة محتملة للهجمات ويتطلب تبني نموذج "عدم الثقة مطلقاً" (Zero-Trust) لحماية الشبكات الداخلية. وعلى مستوى الحلول، خلصت الدراسة إلى مجموعة من أفضل الممارسات الموصى بها: منها اعتماد أطر معيارية معتمدة عالمياً مثل إطار معهد المعايير والتقنية الأمريكي NIST ومعيار ISO/IEC 27001 لضبط سياسات الأمن والإجراءات. فقد بينت دراسات حالة أن تطبيق هذه الأطر المعيارية يُكسب المؤسسات الصحية منهجية واضحة لإدارة المخاطر ويُحسن من موقفها الأمني بشكل ملموس. كذلك أكد على أهمية إجراء تقييمات دورية للمخاطر لاكتشاف

مواطن الضعف الجديدة والتكيف مع التهديدات المستجدة، بالإضافة إلى تدريب العاملين ورفع الوعي الأمني باستمرار لخفض الحوادث الناجمة عن الخطأ البشري. ولم يغفل أهمية خطط الاستجابة للحوادث الجيدة الإعداد، حيث أن وجود خطة استجابة واختبارها دورياً يحدّ بشكل كبير من آثار الاختراق عند حدوثه. وأخيراً، دعا الباحث إلى تعزيز التعاون وتبادل المعلومات بين الجهات الصحية فيما يتعلق بالتهديدات والخبرات، إذ وجد أن تبادل الاستخبارات حول الهجمات وأفضل الممارسات يرفع مناعة القطاع ككل. تُعدّ مساهمة هذه الدراسة (Božić, 2024) مهمة كونها تجمع نتائج عدة دراسات سابقة وتقدّم رؤية تكاملية، لكنها كمراجعة نظرية تظل محدودة بغياب بيانات ميدانية أصلية، كما أنها عامّة النطاق (على مستوى عالمي) ولا تركز تفصيلاً على بيئات إقليمية محددة قد تختلف ظروفها (مثل البيئات العربية). ومع ذلك، فإن توصياتها تُشكل مرجعية قيّمة لتوجيه الدراسات التطبيقية اللاحقة.

من جهة أخرى، هناك دراسات تناولت تحليل حوادث واقعية بهدف استنتاج الدروس المستفادة فيما يخص حماية البيانات الصحية. على سبيل المثال، قام مجموعة من الباحثون بإجراء دراسة (Seh et al., 2020) كمية تحليلية اعتمدت على بيانات موثقة لحوادث اختراق بيانات في القطاع الصحي بالسنوات الأخيرة، بما في ذلك قواعد بيانات خروقات المعلومات وتقارير من هيئات تنظيمية. استخدم الباحثون أساليب إحصائية متقدمة (كنماذج السلاسل الزمنية) لتحليل اتجاهات حوادث اختراق البيانات والتنبؤ المستقبلي بمعدلاتها. وقد أكدت النتائج ما سبق ذكره من أن الهجمات الخارجية (القرصنة الإلكترونية) تشكل النسبة الأكبر من أسباب الخروقات، وأن وتيرة تلك الخروقات في تزايد سريع مع مرور الزمن. كما قدّمت الدراسة تقديرات للتكاليف المالية الناجمة عن تلك الخروقات، مسلّطة الضوء على العواقب الاقتصادية بجانب الأضرار المعنوية. وتكمن قوة هذه الدراسة في اعتمادها على بيانات فعلية واسعة النطاق (من 2005 حتى 2019) مما يجعل استنتاجاتها أكثر موثوقية من الناحية الإحصائية، إضافةً إلى منهجية التنبؤ التي تتيح الاستعداد المسبق للتحديات القادمة. لكن يُلاحظ أن الدراسة تركز على النتائج الكمية للخروقات دون الخوض تفصيلاً في مدى فعالية الضوابط الأمنية المطبقة في المؤسسات محل الدراسة، أي أنها تبين حجم المشكلة وتطورها أكثر مما تقيم نجاح الحلول. كذلك تغطي الدراسة نطاقاً جغرافياً واسعاً (على الأرجح عالمي أو أمريكي) مما قد لا يعكس خصوصيات بعض الدول إلا بشكل عام.

ومع الانتقال إلى الدراسات الأكثر تخصصاً واقترباً من سياق البحث الحالي، نجد جهوداً بحثية قيّمة أُجريت في البيئة الإقليمية (العربية/السعودية) لقياس فاعلية ممارسات الأمن السيبراني في القطاع الصحي. من أبرزها دراسة (Kanaan et al., 2024) وهي دراسة حديثة تناولت القطاع الصحي السعودي وحددت بشكل خاص العلاقة بين استثمارات الأمن السيبراني وإدارة المخاطر التشغيلية من جهة، وإدارة استمرارية الأعمال من جهة أخرى. اعتمد الباحثون منهجية كمية باستخدام الاستبانة الموجهة إلى مديري تقنية المعلومات في عدد من مستشفيات المملكة، ثم قاموا بتحليل البيانات باستخدام نمذجة المعادلات الهيكلية الجزئية (PLS-SEM) للتحقق إحصائياً من العلاقات بين المتغيرات المدروسة. تميزت هذه الدراسة بكونها ميدانية وتحليلية

في آن واحد، إذ اختبرت نموذجاً نظرياً يربط بين الإجراءات التقنية للأمن السيبراني (مثل أنظمة التحكم بالوصول وتشفير البيانات وسلامة البيانات الشبكية) وإدارة المخاطر التشغيلية كمتغير وسيط يؤثر على استمرارية الأعمال في المستشفيات. وقد توصلت الدراسة إلى نتائج مهمة، منها أن تطبيق إجراءات مثل تشفير البيانات وضمان سلامتها كان له الأثر الأقوى في تحسين إدارة المخاطر التشغيلية داخل المستشفيات. وبدوره، أظهرت الدراسة أن نضج إدارة المخاطر التشغيلية ينعكس إيجاباً وبشكل كبير على فاعلية إدارة استمرارية الأعمال، أي أن المستشفيات التي تطبق منهجيات قوية لإدارة المخاطر قادرة بشكل أفضل على الاستمرار في العمل أثناء الأزمات. إضافةً إلى ذلك، بيّنت الدراسة وجود دور وساطة لإدارة المخاطر، حيث تعمل إدارة المخاطر كحلقة وصل تترجم تأثير إجراءات الأمن السيبراني التقنية إلى تحسينات فعلية في مستوى الاستمرارية والمرونة التشغيلية. تسلط هذه النتيجة الضوء على أهمية تكامل الجهود التقنية مع العملية الإدارية، فمجرد الاستثمار في أدوات الأمن لا يكفي لضمان الاستمرارية ما لم يكن هناك إطار شامل لإدارة المخاطر يضمن تفعيل تلك الأدوات وترجمتها إلى سياسات وإجراءات فعّالة. من حيث التقييم، تُعدّ عينة الدراسة (مديرو تقنية المعلومات في عدة مستشفيات سعودية) من نقاط قوتها لأنها تمثل الجهات المعنية مباشرةً بالأمن السيبراني الصحي، كما أن استخدام المنهج الإحصائي المتقدم منح المخرجات مصداقية سببية نسبية. ومع ذلك، قد يشار إلى أن الدراسة اعتمدت على تصورات المشاركين وتقييمهم الذاتي لمستوى الأمن والاستمرارية، مما قد يحمل بعض التحيز أو عدم الدقة. كما أنها ركزت على مستوى إداري محدد، وربما يكون من المفيد في أبحاث قادمة توسيع الاستطلاع ليشمل مستويات وظيفية أخرى (مثل المستخدمين النهائيين من الطاقم الطبي) أو قياس الأثر الفعلي على مؤشرات رقمية للأداء (مثل عدد الحوادث الأمنية أو مدة تعطل الأنظمة).

وفي سياق قريب، أجرت وزارة الصحة في إيران تقييماً ميدانياً واسع النطاق يمكن مقارنته بالسياق السعودي من حيث طبيعة النظم الصحية. قامت الوزارة عبر فرق مختصة بتنفيذ مسح شامل على مستوى 551 مستشفى في مختلف أنحاء إيران، بهدف تقييم وضع إدارة أمن المعلومات والمخاطر السيبرانية في تلك المستشفيات وشمل التقييم جوانب عدة مثل وجود سياسات أمنية، وتطبيق نظم إدارة أمن المعلومات (ISMS)، وإجراءات تحديد المخاطر وتقييمها، وخطط حماية الخصوصية. رسمت نتائج الدراسة (Mirzaei et al., 2020) صورة مختلطة: فمن جهة، نحو 69% من المستشفيات أفادوا بتطبيقهم نظام إدارة لأمن المعلومات وفق معايير معتمدة، مما يوحي بانتشار الوعي بالمتطلبات التنظيمية الأساسية. لكن في المقابل، تبين أن عمليات تحديد المخاطر وتقييمها تقتصر إلى التنظيم والمنهجية في عدد كبير من تلك المستشفيات، حيث لوحظ أن كثيراً من المرافق تعتمد ممارسات ارتجالية أو غير موثقة لتقييم المخاطر، بدلاً من اتباع نهج موحد ومستدام. هذا القصور في منهجية إدارة المخاطر – رغم توفر البنى والسياسات – يشير إلى فجوة بين إقرار أهمية الأمن السيبراني وترجمتها فعلياً إلى إجراءات تشغيلية على أرض الواقع. تميز هذا التقييم بحجم عينته الكبير التي تشمل قطاعاً صحياً وطنياً كاملاً، مما يضفي موثوقية على مخرجاته ويجعلها قاعدة للمقارنة مع دول أخرى. ومع ذلك فإن تفاصيله الدقيقة قد لا تكون منشورة في دوريات علمية محكمة

بالطريقة التقليدية (كونه صادر عن جهة حكومية)، كما قد تختلف البيئة الإيرانية تنظيمياً وتقنياً عن البيئة السعودية. لكن يبقى الاستنتاج الأساسي قابلاً للاعتبار: وجود حاجة لوضع أطر عمل أكثر وضوحاً لتنفيذ إدارة المخاطر في المستشفيات، وليس فقط تبني سياسات شكلية.

ضمن الجهود البحثية ذات الصلة الوثيقة بالعامل البشري في الأمن السيبراني الصحي، برزت دراسة (Rizzoni et al., 2022) التي نفذت ثلاث حملات محاكاة تصيد احتيالي على مدى عام في مستشفى إيطالي يضم أكثر من 6 آلاف موظف. أظهرت النتائج أنَّ نسبة النقر على الروابط الخبيثة في الرسائل «المعيارية» انخفضت من 18 % في الحملة الأولى إلى 7 % في الحملة الثالثة، كما تراجعَت النسبة في الرسائل «المُخصَّصة» من 55 % إلى 21 %، وهو ما يعكس أثراً إيجابياً ملموساً للتدريب المصحوب بالتغذية الراجعة على رفع يقظة العاملين وتقليل الأخطاء البشرية المرتبطة بالتصيد.

وفي سياقٍ عربي، قدَّمت الدراسة (Alhuwail et al., 2021) مسحاً على 453 من العاملين في مرافق صحية كويتية، كاشفةً أن الممارسة الآمنة للمعلومات ترتبط بعوامل ديموغرافية؛ حيث تفوق الممرضون على الأطباء في التزامهم بسلوكيات الأمن السيبراني، وأوصى الباحثون ببرامج تدريب مُوجَّه تستهدف الفئات الأكثر عُرضة للمخاطر.

تتقاطع هذه النتيجة مع ما توصلت إليه الدراسة (Dawood Ahmed Rihan, 2025) في السياق السعودي الأكاديمي، حيث درست مستوى الوعي والتحديات في تبني الأمن السيبراني لدى منسوبي كليات صحية في جامعة نجران. على الرغم من أن تلك الدراسة تركز على بيئة تعليمية، فإن نتائجها تعطي مؤشراً عن واقع الوعي الأمني في قطاع مرتبط بالصحة في منطقة نجران. اعتمدت ريهان منهجية وصفية تحليلية باستبانة لقياس وعي أعضاء هيئة التدريس والموظفين بمفاهيم الأمن السيبراني ومخاطره وأساليب انتهاكه. وقد وجدت الدراسة أن هناك مستوى وعي مرتفع نسبياً بالمفاهيم الأساسية والمخاطر السيبرانية لدى المشاركين (تراوح متوسط التقييم بين 4.00 و4.06 من 5)، مما يشير إلى إدراك عام جيد لمخاطر الأمن السيبراني ووجود اتجاهات إيجابية نحو الالتزام بإجراءات الحماية. ومع ذلك أبرزت الدراسة حاجة ملحة لوضع خطة أمن سيبراني شاملة لتعزيز المنظومة الحالية، فلا يكفي الوعي النظري لدى الأفراد ما لم يترجم إلى سياسات وإجراءات مؤسسية. وأشارت في خلاصتها إلى أن مجرد المعرفة بالأنظمة والقوانين لا يغني عن بناء قدرات مؤسسية واستراتيجية أمنية محكمة. وتوصي بأن تشمل الجهود المستقبلية عناصر متنوعة (تقنية وبشرية وإدارية) لضمان بيئة تعليمية وصحية أكثر أماناً. يُذكر أن عينة هذه الدراسة كانت من الوسط الأكاديمي الصحي، ما قد يجعل تعميم نتائجها على المستشفيات بحاجة إلى حذر، لكنّها تكشف جانباً مهماً هو توفر الوعي النظري لدى الكوادر الصحية السعودية مع وجود تحديات في تحويل هذا الوعي إلى ممارسات فعالة.

أخيراً، تجدر الإشارة إلى دراسة نوعية حديثة أجريت في أستراليا تطرقت بشكل غير مباشر لموضوع فعالية إدارة مخاطر الأمن السيبراني ولكن من زاوية مختلفة، حيث درست أفضل السبل لتعزيز جاهزية القطاع الصحي لمواجهة التهديدات. قام الباحثون القائمون على الدراسة (Burke et al., 2024) بإجراء مجموعات

تركيز شملت خبراء من قطاع الرعاية الصحية والأمن السيبراني، وجرى تحليل مناقشاتهم لاستنباط المحاور الرئيسية التي يرونها تحديات أو أولويات. من بين أبرز النتائج كانت الإشارة إلى عدم وضوح أفضل الممارسات الواجب اتباعها في القطاع الصحي رغم ازدياد الهجمات، خاصة أن المستشفيات تواجه تحديات مالية وتقنية تجعل تبني حلول الأمن أمراً معقداً. حدد الخبراء أربعة محاور أساسية ينبغي التركيز عليها : تأمين البنية الصحية المعقدة، التحديات المالية في تمويل أمن المعلومات، الموازنة بين خصوصية البيانات وشفافية المعلومات في الرعاية الصحية، وأخيراً دور التعليم واللوائح التنظيمية. وكان من أهم التوصيات التي خرجت بها هذه الدراسة هو الحاجة إلى أدوات تقييم ذاتي خاصة بقطاع الصحة تساعد المؤسسات الصحية على تقييم نقاط الضعف بشكل استباقي. حيث شعر الخبراء أن كثيراً من الجهود تتركز على رد الفعل بعد وقوع الحوادث، في حين أن هناك نقصاً في الأدوات أو النماذج التي تمكن المستشفيات من تحديد مكان الضعف قبل استغلالها. هذه الخلاصة تمثل فجوة بحثية تستدعي الانتباه، إذ على الرغم من كثرة الأبحاث حول أمن المعلومات الصحي، إلا أن المنهجيات الاستباقية (مثل التقييم الذاتي المنتظم والاختبارات الدورية للأنظمة) لا تزال غير مطورة بما يكفي حسب رأي الخبراء. ميزة هذه الدراسة أنها توفر رؤية نوعية معمقة من واقع خبراء الممارسة، مما يضيف مصداقية عملية على الفجوات المحددة. لكن محدوديتها تكمن في حجم العينة الصغير (خمس خبراء فقط) وطبيعة النتائج التي قد تكون خاصة بالسياق الأسترالي. ومع ذلك، فإنها تثير تساؤلاً مهماً له صلة بموضوع البحث: إلى أي مدى المؤسسات الصحية مستعدة بشكل استباقي لتقييم وإدارة مخاطر الأمن السيبراني قبل حدوث الكارثة؟.

تحليل الدراسات السابقة

من خلال الاستعراض السابق للدراسات المرجعية يمكن استخلاص رؤى مشتركة ومحاور محورية تبلورت عبر تلك الأدبيات، وكذلك تحديد الفجوات البحثية التي ما زالت قائمة والتي يمهّد تحديدها لبلورة مساهمة البحث الحالي. يوضح الجدول (جدول 1) تلخيصاً موضوعياً مقارناً لأبرز النتائج من الدراسات السابقة، مجمّعة حسب محاور التركيز الرئيسية:

جدول 1: جدول مقارنة - أبرز نتائج الدراسات السابقة

المحور الرئيسي	الدراسات البارزة	أبرز النتائج والملاحظات
أطر إدارة المخاطر ومعايير الأمن	(Božić, 2024) (Kanaan et al., 2024) (Mirzaei et al., 2020)	- اعتماد أطر معيارية (مثل NIST و ISO 27001) يوفر نهجاً منهجياً لتحسين الوضع الأمني وإدارة المخاطر في المستشفيات. - وجود نظام إدارة أمن معلومات (ISMS) شائع في العديد من المستشفيات (69% في إيران) لكن منهجية تقييم المخاطر قد تكون غائبة أو غير منتظمة. - تؤكد دراسات متعددة أن الجمع بين الامتثال للمعايير والتنفيذ الفعلي لإدارة المخاطر هو ما يحقق الحماية الفعالة، إذ لا يكفي الالتزام النظري ما لم تصحبه إجراءات تقييم ومراجعة مستمرة للمخاطر.
التدابير التقنية لحماية البيانات	(Pool et al., 2024) (Seh et al., 2020) (Kanaan et al., 2024)	- هناك إجماع على أن الإجراءات التقنية الصارمة ضرورية لحماية بيانات المرضى: مثل التشفير القوي للبيانات الحساسة وتقييد صلاحيات الوصول وأنظمة المراقبة والتدقيق المستمر. - تُظهر البيانات أن الهجمات الإلكترونية الخارجية تشكل الخطر الأكبر على البيانات الصحية، مما يجعل تعزيز الضوابط التقنية أولوية. كما أن بعض الدراسات نبهت إلى التهديدات الداخلية (كإفشاء البيانات من الداخل)، مما يعني الحاجة إلى ضوابط تشمل مراقبة تصرفات المستخدمين المصرح لهم أيضاً. - وجدت الدراسات أن ضمان سلامة البيانات (integrity) وتشغيلها من أكثر العوامل تأثيراً على نجاح إدارة المخاطر، مما يدعم ما جاء في دراسات سابقة من أهمية الدور المحوري للتقنية في منظومة الأمن.
العوامل البشرية والتوعية	(Rizzoni et al., 2022) (Alhuwail et al., 2021)	التوعية والتدريب عنصران حاسمان: تدريب الموظفين دورياً على مبادئ الأمن السيبراني يقلل الحوادث الناجمة عن الخطأ البشري بشكل ملحوظ. كما أن رفع الوعي الأمني لدى الكوادر الصحية (كما في دراسة نجران) يشكل خطوة إيجابية لكنه بحاجة لدعم بخطط وإجراءات ملموسة.

• ثقافة الأمن المؤسسية مهمة في تشكيل سلوك العاملين: إذ أشارت بعض الدراسات إلى أن وجود سياسة أمنية واضحة وثقافة داعمة يقلل من التساهل ويعزز الالتزام (مثل دراسة مناخ الأمن التي وجدت ارتباطاً بين سياسات الشركة وسلوك الموظفين). • مع أن مستوى الوعي النظري بالمخاطر قد يكون مرتفعاً، إلا أن ترجمته إلى ممارسات ليست مضمونة دائماً – ما لم يكن هناك التزام إداري وتدريب مستمر. وقد ظهر تباين في بعض النتائج: فمثلاً، ورغم وعي العاملين العالي في حالة جامعة نجران، أظهر تقييم آخر أن بعض الفئات (كالصيادلة في دراسة مناخ الأمن) قد يكونون أقل إدراكاً للمخاطر مقارنة بزملائهم، مما يستدعي نهجاً موجهاً لكل فئة في التدريب والتوعية.	Dawood Ahmed) (Rihan, 2025	
• تكامل إدارة المخاطر مع استمرارية الأعمال أثبتت فعاليتها: حيث تبين أن وجود إطار قوي للمخاطر (ORM) يؤدي إلى تعزيز قدرة المستشفى على الصمود أثناء الأزمات. • الهجمات السيبرانية تهدد بشكل مباشر استمرارية الخدمات الصحية: ظهر ذلك جلياً في حادثة WannaCry وغيرها، حيث تسببت في إلغاء مواعيد وتأجيل عمليات وتحويل مرضى، ما أكد أن الأمن السيبراني ليس مجرد قضية تقنية بل مرتبط باستمرار الرعاية الصحية وسلامة المرضى. • خطط الاستجابة للحوادث والطوارئ تعد جزءاً أساسياً من معادلة المرونة. بينت بعض الدراسات أن المستشفيات التي لديها خطط مدروسة ومختبرة كانت أسرع تعافياً وأقل ضرراً عند حدوث خرق أمني researchgate.net. ومع ذلك، هناك دليل على أن العديد من المؤسسات الصحية لم تختبر خططها دورياً أو تراجعها، مما يمثل ثغرة يمكن أن تؤثر على فعاليتها وقت الأزمة. • إجماع الخبراء (بورك وآخرون) يشير إلى الحاجة لأدوات تقييم استباقية للجاهزية، بحيث لا يقتصر الأمر على رد الفعل، بل يتم قياس نقاط الضعف ومعالجتها قبل أن تتسبب في انقطاع الخدمة.	(Kanaan et al., 2024) (Burke et al., 2024)	استمرارية الخدمة والمرونة التشغيلية

من الجدول والتحليل في الجدول (جدول 1)، يمكن تلمّس عدد من الاتجاهات العامة في الأدبيات السابقة. أولها وجود توافق عام على ضرورة النهج الشمولي في إدارة مخاطر الأمن السيبراني بالقطاع الصحي، أي التكامل بين العناصر التقنية (الأدوات والضوابط) والعناصر التنظيمية/البشرية (السياسات والتدريب والثقافة المؤسسية). فمعظم الدراسات تؤكد أن علاج جانب واحد وإهمال الآخر يقلل من فعالية الجهود المبذولة. فعلى سبيل المثال، أظهرت دراسات الامتثال التنظيمي (مثل دراسة (Lim et al., 2019) المشار إليها في مراجعة (Božić, 2024)) أن الالتزام بالمعايير مثل HIPAA و GDPR يساهم في حماية البيانات وبناء الثقة مع المرضى، لكنه وحده غير كافٍ ما لم يتم تنبيه ضمن استراتيجية أمنية أوسع نطاقاً تشمل إدارة أنشطة للمخاطر والتحديث المستمر للإجراءات. وهذا يتفق مع ما أشارت إليه دراسة إيران الميدانية من وجود سياسات على الورق دون تفعيل كامل في الممارسة. ومن الاتجاهات المشتركة أيضاً التأكيد على ارتفاع وتيرة تهديدات الأمن السيبراني الصحية في السنوات الأخيرة، مما يجعل الحاجة ماسة لتقييم مدى جاهزية المؤسسات الصحية. ورغم أن الدراسات وثقت بوضوح تصاعد الهجمات وتقنيات الاختراق (خصوصاً مع رقمنة السجلات الصحية والانتشار الكبير للأجهزة الذكية المتصلة)، إلا أن جانب قياس الفعالية – أي مدى نجحت التدابير الحالية في الحد من تلك الهجمات أو تخفيف أثرها – لم يحظ بالقدر نفسه من البحث التجريبي. فقد ركزت كثير من الدراسات إما على توصيف المشكلة (حجم الخروقات وأنواعها) أو اقتراح الأطر النظرية للحل، دون تقييم كمي أو نوعي لمدى كفاءة ممارسات محددة على أرض الواقع. على سبيل المثال، لا تزال هناك محدودية في الدراسات التي تربط بين مستوى تبني إطار أمن معين وانخفاض حقيقي في عدد حوادث الاختراق داخل مؤسسة ما. أيضاً، برز تباين في تركيز الدراسات: بعضها انصب على حماية البيانات كغاية أساسية، وأخرى على استمرارية العمليات، وثالثة على الثقافة التنظيمية، وهذا يعكس تشعب الموضوع. إلا أن البحث الحالي يجمع هذه الأبعاد معاً تحت مظلة سؤال واحد، ما يتطلب سد الفجوة بين هذه الاتجاهات المنفصلة.

من ناحية أخرى، كشفت المراجعة عن فجوات وتناقضات تستوجب الدراسة. من أهمها نقص الأبحاث في السياق المحلي والعربي، إذ رغم توفر بعض الدراسات في السعودية (مثل: (Kanaan et al., 2024)، (Dawood Ahmed Rihan, 2025))، يظل العدد محدوداً ولا يغطي كافة جوانب المشكلة. البيئة التنظيمية والتقنية في المملكة لها خصوصيتها (مثل وجود هيئة وطنية للأمن السيبراني، وتشريعات خاصة لحماية البيانات الصحية) مما يستدعي أبحاثاً تستكشف فاعلية الممارسات ضمن هذا الإطار المحلي. كذلك، برز تباين في النتائج يتعلق بالعامل البشري: فبينما أكدت دراسات على فعالية التدريب، أظهرت أخرى أن الوعي وحده قد لا يغيّر السلوك بالضرورة. هذا يطرح تساؤلاً حول كيفية قياس وتحسين الثقافة الأمنية داخل المؤسسات الصحية – وهي مسألة لم تحسمها الأدبيات بعد بشكل عملي. إضافة لذلك، هناك فجوة تتعلق بالنهج الاستباقي كما أشار الخبراء الأستراليين، فمعظم تركيز المؤسسات (وبالتالي البحوث) كان على

التصدي والتعافي بعد وقوع الهجوم، في حين أن مفاهيم التقييم الذاتي المستمر والمراجعة الاستباقية للمخاطر لا تزال غير متطورة بما يكفي في التطبيق (ربما لصعوبة قياسها أو غياب أدوات قياسية واضحة).

بناءً على ما سبق، يتميز البحث الحالي بأنه يأتي استجابةً مباشرةً لهذه الفجوات: فهو يركز على تقييم فاعلية ممارسات الأمن السيبراني، وليس مجرد رصد وجودها من عدمه، وفي سياق محلي (تجمع صحي في نجران) لم يُدرس بعمق من قبل. كما أنه ينظر بعين متوازنة إلى حماية البيانات واستمرارية الخدمة كهدفين متلازمين، أخذاً بالاعتبار العوامل التقنية والتنظيمية والبشرية جميعاً. هذه النظرة التكاملية تُهيئ الفرصة لسد ثغرات الدراسات السابقة التي عالجت كل جانب بمعزل نسبي عن الآخر.

في الختام، وفي ضوء الاستعراض والتحليل أعلاه، يتضح أن الدراسات السابقة - رغم غناها بالأفكار والمعطيات - لم تغطِّ بعدُ جميع جوانب مشكلة البحث الراهن. فقد تناولت كل منها أجزاءً من الصورة الكلية: فبعضها ركز على أهمية الأطر والسياسات، وأخرى على التقنيات أو التدريب، وقليل منها حاول الربط بين تلك المكونات وقياس الأثر الفعلي على النتائج الملموسة كسلامة البيانات واستمرارية الخدمات. كما برز نقص في الأبحاث الميدانية ضمن السياق السعودي local/رغم الاعتراف العالمي بتزايد التهديدات السيبرانية في قطاع الصحة. هذه الثغرات هي ما يُبرّر بوضوح الحاجة إلى الدراسة الحالية. فهي محاولة لسد فراغ معرفي من خلال تقييم شمولي وميداني لفاعلية ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات المرضى وضمان استمرار الخدمات الصحية في بيئة محلية محددة. وبذلك، سيسهم البحث في تطوير المعرفة العلمية عبر تزويد صانعي القرار في القطاع الصحي بمؤشرات مبنية على أدلة حول أي الممارسات أنجع تأثيراً، وأين تكمن نقاط الضعف التي تتطلب معالجة. ومن ثم، يمثل هذا العمل لبنة مكملة لجهود الدراسات السابقة، حيث يبني على ما وصلوا إليه ويتجاوز ما لم يتمكنوا من تغطيته، آمليين أن تسد نتائجُه الفجوة بين التوصيات النظرية والتطبيق العملي في ميدان أمن المعلومات الصحي.

الإطار النظري للدراسة

ترتكز هذه الدراسة على إطار نظري متين يستند إلى مفاهيم إدارة المخاطر والأمن السيبراني في قطاع الرعاية الصحية. تعد إدارة مخاطر الأمن السيبراني عملية منظمة تهدف إلى تحديد التهديدات وتحليلها واتخاذ تدابير لحماية الأصول الحرجة (كالأنظمة والبيانات) من نطاق واسع من المخاطر المحتملة. في مجال الرعاية الصحية، يكتسب هذا الإطار أهمية مضاعفة نظراً لحساسية بيانات المرضى وتأثير أي اختراق أمني على سلامة المرضى وجودة الرعاية المقدمة. وقد أشارت الدراسات الحديثة إلى أن إدارة المخاطر الفعالة قد تكون الفارق بين الحياة والموت في البيئات الصحية الرقمية (Molosiwa & Molosiwa, 2025)، إذ يؤدي أي فشل في حماية البيانات أو توفير الخدمات إلى عواقب جسيمة.

أهداف إدارة المخاطر السيبرانية في الرعاية الصحية: تتسق أهداف إدارة المخاطر في المجال الصحي مع ثلاثة محاور رئيسية: (1) حماية بيانات المرضى وسجلاتهم من الوصول غير المصرح والافشاء غير القانوني، (2) تحسين قدرة المنظمة على التعرف على الثغرات والتهديدات السيبرانية ضمن بنيتها التقنية بشكل استباقي، و (3) ضمان استمرارية الأعمال والخدمات الصحية وسلامة المرضى حتى في حال وقوع هجوم أو كارثة رقمية. ويعكس الهدف الأخير جوهر مفهوم استمرارية الخدمة أو استمرار الرعاية، حيث تسعى المؤسسات الصحية إلى وضع خطط طوارئ واستجابة فعالة تمكنها من العودة إلى العمل الطبيعي بأسرع وقت ممكن بعد الحوادث السيبرانية.

أهمية الأمن السيبراني لحماية بيانات المرضى واستمرارية الخدمات: تتجلى أهمية تبني ممارسات قوية للأمن السيبراني في المؤسسات الصحية من خلال القدرة على منع حوادث اختراق البيانات وتعطيل الخدمات. فالمعلومات الصحية الإلكترونية (مثل السجلات الطبية) تحتوي على بيانات شخصية وتاريخ مرضي ومالية تجعلها من أكثر البيانات حساسية. إن حماية سرية وسلامة وتوافر هذه المعلومات ليست مجرد قضية تقنية، بل هي أيضاً مطلب قانوني وأخلاقي تفرضه التشريعات والمعايير الدولية، حيث يلزم مؤسسات الرعاية الصحية الامتثال لاشتراطات أمنية مثل قانون HIPAA في الولايات المتحدة واللائحة GDPR في الاتحاد الأوروبي بهدف ضمان سرية وسلامة وتوافر المعلومات الصحية الإلكترونية. إخفاق أي منشأة صحية في حماية بيانات مرضاها قد يعرضها لعقوبات قانونية وخسائر مالية بالإضافة إلى فقدان ثقة المجتمع بها. ومن ناحية أخرى، فإن تعطل الخدمات الصحية نتيجة هجوم سيبراني كفيل بتقويض سلامة المرضى بشكل مباشر، فقد أفادت تقارير عن حوادث حقيقية كتعطل مستشفيات وإلغاء عمليات جراحية نتيجة هجمات فدية رقمية. لذا، أصبح يُنظر إلى الأمن السيبراني على أنه جزء لا يتجزأ من سلامة المرضى واستدامة الرعاية الصحية. توصي الأدبيات بضرورة دمج اعتبارات الأمن السيبراني ضمن أطر حوكمة وإدارة المخاطر واستمرارية الأعمال في المؤسسات الصحية، بحيث يصبح التعامل مع المخاطر الرقمية مسؤولية إدارية واستراتيجية تشارك فيها كافة المستويات التنظيمية وليس مجرد شأن تقني.

ممارسات وأطر إدارة مخاطر الأمن السيبراني: طورت الأطر العالمية أفضل الممارسات لمساعدة المؤسسات على إدارة المخاطر السيبرانية بفعالية. من أبرز تلك الأطر إطار عمل NIST للأمن السيبراني ومعايير ISO/IEC 27000، والتي توفر إرشادات منهجية لتحديد الأصول الحيوية والتهديدات، وتقييم نقاط الضعف، وتطبيق ضوابط الحماية الملائمة، ورصد الامتثال والتهديدات بشكل مستمر. تشمل الممارسات الشائعة في هذا السياق: تقييم المخاطر الدوري لتقدير احتمالية حدوث التهديد وتأثيره، تطبيق إجراءات الحماية التقنية مثل التشفير ومصادقة متعددة العوامل وتحديث البرمجيات باستمرار، التوعية والتدريب الأمني لبناء ثقافة داخلية قوية قادرة على التصدي للهندسة الاجتماعية وتقليل الأخطاء البشرية، إدارة صلاحيات الوصول لضمان أن يمتلك كل مستخدم أقل قدر ممكن من الحقوق وفقاً لمبدأ الحاجة للاطلاع، وكذلك خطط الاستجابة للحوادث والتعافي التي تضمن جاهزية المؤسسة للتحرك السريع عند وقوع اختراق واحتواء الضرر واستعادة الخدمات. كما تتضمن الممارسات المتقدمة إدارة مخاطر الأطراف الخارجية (كالشركات الموردة للخدمات التقنية) عبر التحقق من امتثالها للمعايير الأمنية، نظراً لأن ضعف أمن الموردين قد يشكل ثغرة خطيرة للمؤسسة الصحية. أخيراً، تشدد الأدبيات على المراقبة المستمرة لمشهد المخاطر السيبرانية، نظراً للطبيعة المتطورة للهجمات، بحيث يجري تحديث سياسات وإجراءات الأمن دورياً ومراجعة كفاءة الضوابط الأمنية باستمرار.

بناءً على ما سبق، يستند الإطار النظري لهذه الدراسة إلى حقيقة أن إدارة المخاطر السيبرانية الفعالة في القطاع الصحي هي شرط أساسي لحماية خصوصية المرضى وضمان استمرارية الخدمات الصحية دون انقطاع. وسوف تعتمد الدراسة على دمج المعايير والممارسات الدولية مع واقع بيئة تجمع نجران الصحي لتحليل نقاط القوة والضعف في ممارسات الأمن السيبراني الحالية، وذلك على ضوء الأبحاث السابقة والمفاهيم النظرية الراسخة في هذا المجال.

الفصل الثالث: منهجية الدراسة

مقدمة

يستعرض هذا الفصل الإجراءات المنهجية التي اتُبعت في تنفيذ هذه الدراسة، بهدف تقييم فاعلية ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات المرضى وضمان استمرارية الخدمات الصحية في تجمع نجران الصحي. تعتمد الدراسة منهجية علمية منظمة تمكّن من جمع بيانات دقيقة وموثوقة، وتحليلها بأساليب إحصائية ملائمة للوصول إلى نتائج قابلة للتعميم ضمن السياقات المماثلة.

تكتسب منهجية البحث أهميتها من كونها الإطار الذي يحكم مصداقية النتائج وموثوقيتها (Creswell & Creswell, 2023). فالمنهجية السليمة تضمن أن تكون الاستنتاجات مبنية على أدلة تجريبية صلبة وليست انطباعات ذاتية، وهو ما يتوافق مع المعايير الأكاديمية العالمية في البحوث الصحية والإدارية (Saunders et al., 2023). يغطي هذا الفصل تصميم البحث، مجتمع الدراسة وعينتها، أدوات جمع البيانات وإجراءاتها، حدود الدراسة، بالإضافة إلى أساليب التحليل الإحصائي المستخدمة.

يتبنى الباحث المنهج الوصفي التحليلي (Descriptive-Analytical Approach) كإطار منهجي شامل، وهو منهج يتيح وصف الظاهرة محل الدراسة كما هي في الواقع، ثم تحليل مكوناتها وعلاقاتها بهدف فهم أعمق للعوامل المؤثرة فيها (Kumar, 2019). يُستخدم هذا المنهج على نطاق واسع في دراسات إدارة المخاطر والأمن السيبراني في القطاع الصحي، حيث يسمح بالربط بين الجانبين الكمي والنوعي للظاهرة (Whitman & Mattford, 2019).

تصميم البحث

يعتمد هذا البحث على تصميم منهجي مُحكم يتدرّج عبر مراحل مترابطة تهدف إلى بناء معرفة علمية دقيقة حول فاعلية ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات المرضى وضمان استمرارية الخدمات الصحية في تجمع نجران الصحي. تبدأ المرحلة الأولى بتحديد مشكلة البحث وصياغة أسئلته الرئيسية والفرعية استناداً إلى واقع القطاع الصحي السعودي ومتطلبات الأمن السيبراني الوطني. يلي ذلك مراجعة الأدبيات والمصادر العلمية بهدف تحديد النظريات المناسبة، ورصد الجهود السابقة، واكتشاف الفجوات البحثية التي تستدعي المعالجة.

بعد ذلك تأتي مرحلة تصميم المنهجية، حيث يتم تحديد مجتمع الدراسة وعينتها، وتطوير أداة القياس (الاستبانة)، والتحقق من صدقها وثباتها. ثم تُنفَّذ مرحلة جمع البيانات الميدانية عبر توزيع الاستبانة إلكترونياً على الفئة المستهدفة داخل المؤسسات الصحية، ثم تنقيتها والتأكد من جودتها وصلاحياتها للتحليل. تليها المرحلة التحليلية التي يُستخدم فيها SPSS لتطبيق الأساليب الإحصائية الوصفية والاستنتاجية بما يسمح

بفحص الفرضيات وتفسير العلاقات بين المتغيرات. وتنتهي عملية البحث بمرحلة مناقشة النتائج واستخلاص التوصيات العملية والعلمية في ضوء الأدبيات والممارسات الفضلى. ويوضح الشكل (شكل 1) المراحل المتسلسلة لتصميم البحث:



شكل 1: مخطط مراحل تصميم البحث

النموذج المفاهيمي للبحث

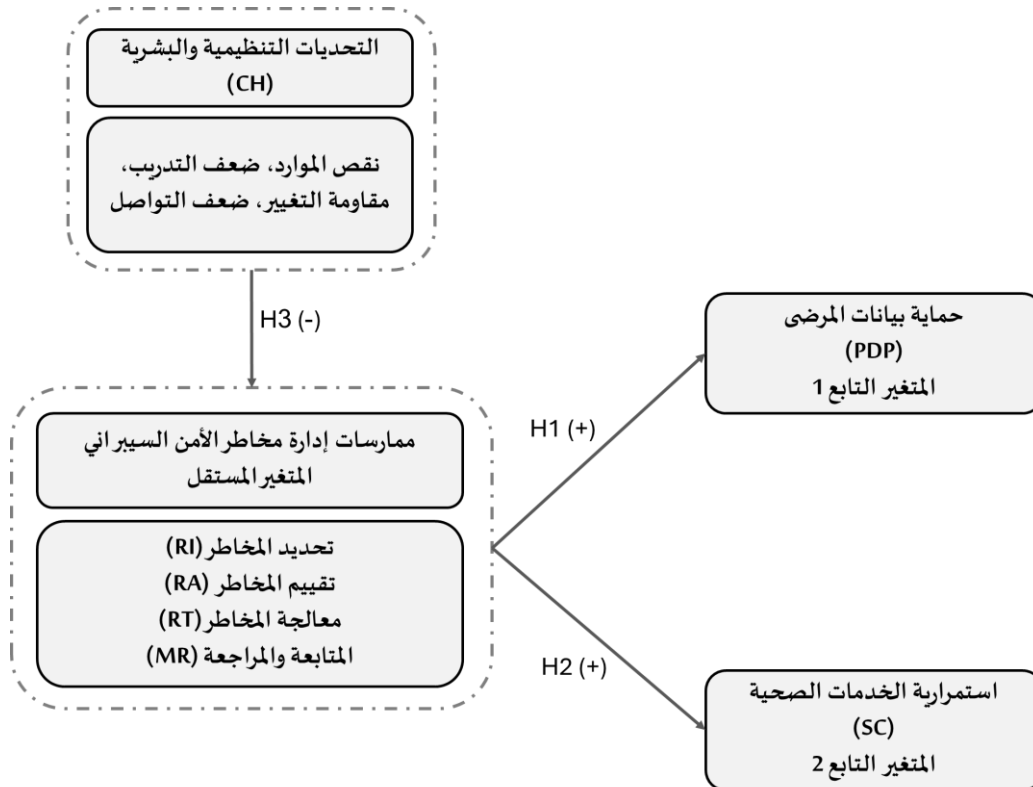
يعتمد هذا البحث على نموذج مفاهيمي يوضح طبيعة العلاقات المتوقعة بين المتغيرات الرئيسية للدراسة، ويتسق مع المعايير الدولية المعتمدة في إدارة مخاطر الأمن السيبراني داخل القطاع الصحي. يفترض النموذج أن ممارسات إدارة مخاطر الأمن السيبراني—بوصفها المتغير المستقل—تمثل منظومة متكاملة تستند إلى أربعة أبعاد مترابطة: تحديد المخاطر (Risk Identification)، تقييم المخاطر (Risk Assessment)، معالجة المخاطر (Risk Treatment)، ومتابعة ومراجعة المخاطر (Monitoring & Risk Assessment).

(Review). وتشكل هذه الأبعاد معاً الإطار المنهجي الذي تطبقه المؤسسات الصحية لضمان أمن المعلومات واستمرارية الأداء التشغيلي.

ويبين النموذج أن فعالية تطبيق هذه الأبعاد من شأنه أن ينعكس إيجاباً على مستويين أساسيين من نتائج الأمن السيبراني في المنشآت الصحية، هما: حماية بيانات المرضى (Patient Data Protection) واستمرارية الخدمات الصحية (Service Continuity). إذ يُتوقع أن يسهم التطبيق المنهجي لممارسات إدارة المخاطر في الحد من فرص حدوث الاختراقات أو التسريبات، وتعزيز قدرة الأنظمة والخدمات الصحية على الصمود أمام الهجمات السيبرانية وتقليل فترات التعطل.

كما يفترض النموذج وجود تحديات تنظيمية وبشرية—مثل محدودية الموارد، ونقص الكفاءات المتخصصة، وضعف التدريب والوعي الأمني، ومقاومة التغيير التقني—تعمل بوصفها عاملاً مؤثراً سلبياً قد يحد من قدرة المؤسسات الصحية على تطبيق الممارسات المثلى لإدارة المخاطر بالشكل الذي يحقق أهداف الحماية والاستمرارية. ومن ثم، فإن النموذج يطرح علاقات تأثير رئيسية بين المتغيرات، إضافةً إلى تأثير معيقي قد يمارسه المتغير التنظيمي-البشري على هذه العلاقات.

ويمثل هذا النموذج الأساس الذي انطلقت منه فرضيات الدراسة المتعلقة بتأثير ممارسات إدارة مخاطر الأمن السيبراني في حماية بيانات المرضى واستمرارية الخدمات، وكذلك أثر التحديات التنظيمية والبشرية في هذه العلاقة. ويوضح الشكل المفاهيمي (شكل 2) طبيعة هذه العلاقات واتجاهاتها.



شكل 2: النموذج المفاهيمي للبحث

المنهج البحثي

تتبع هذه الدراسة المنهج الوصفي التحليلي (Descriptive-Analytical Method)، وهو أحد أكثر المناهج البحثية ملاءمة لدراسة الظواهر الإدارية والتنظيمية في بيئتها الطبيعية. يُعرّف المنهج الوصفي التحليلي بأنه "منهج يقوم على جمع البيانات والمعلومات عن ظاهرة معينة ووصفها وتحليل خصائصها وعلاقاتها بهدف الوصول إلى استنتاجات تساعد في فهم الواقع وتطويره (Sekaran & Bougie, 2016). يوفر هذا المنهج عدة مزايا للدراسة الحالية:

أولاً، يتيح وصفاً دقيقاً لواقع ممارسات إدارة المخاطر السيبرانية في تجمع نجران الصحي من خلال جمع بيانات كمية قابلة للقياس حول مستوى تطبيق الضوابط الأمنية، مما يوفر صورة واضحة عن الوضع الراهن (Creswell & Creswell, 2023).

ثانياً، يمكن من تحليل العلاقات بين المتغيرات المختلفة، مثل العلاقة بين مستوى تطبيق السياسات الأمنية وبين معدل حوادث الاختراق، أو بين كفاءة البنية التحتية التقنية واستمرارية الخدمات الصحية (Field, 2013).

ثالثاً، يسمح باختبار الفرضيات البحثية بطريقة موضوعية من خلال استخدام الأساليب الإحصائية الاستدلالية، مما يعزز من موثوقية النتائج (Kumar, 2019).

تشير الأدبيات الحديثة إلى أن المنهج الوصفي التحليلي يُستخدم بفعالية في دراسات الأمن السيبراني الصحي، حيث وظفته دراسة (Kruse et al., 2017) في تحليل حوادث الأمن السيبراني في المؤسسات الصحية الأمريكية، كما استخدمته دراسة (Luna et al., 2016) في تقييم آليات الاستجابة للحوادث السيبرانية في المستشفيات.

نوع البحث

تُصنف هذه الدراسة ضمن البحوث الميدانية التطبيقية (Applied Field Research)، حيث تهدف إلى دراسة مشكلة واقعية في بيئة عملية محددة (تجمع نجران الصحي) بهدف تقديم حلول عملية قابلة للتطبيق. تختلف البحوث التطبيقية عن البحوث الأساسية (Basic Research) في كونها موجهة نحو معالجة مشكلات محددة في سياقات عملية، بدلاً من بناء نظريات عامة (Saunders et al., 2023). يتوافق هذا التصنيف مع طبيعة المشكلة البحثية، حيث تسعى الدراسة إلى تقييم فاعلية الممارسات الحالية وتقديم توصيات قابلة للتنفيذ من قبل إدارة التجمع الصحي لتعزيز مستوى الأمن السيبراني وحماية بيانات المرضى.

استراتيجية البحث

تعتمد الدراسة على استراتيجية المسح (Survey Strategy) كاستراتيجية بحثية رئيسية. يُعرّف المسح بأنه "أسلوب منهجي لجمع البيانات من عينة كبيرة نسبياً من المجتمع المستهدف باستخدام أدوات موحدة، بهدف وصف الخصائص أو الآراء أو السلوكيات" (Archer, 2023).

تتميز استراتيجية المسح بعدة خصائص تجعلها مناسبة للدراسة الحالية: (Creswell & Creswell, 2023)

- **وحدة المعيار (Standardization):** تطرح نفس الأسئلة على جميع المشاركين بنفس الطريقة، مما يقلل من التحيز ويزيد من موثوقية المقارنات.
- **الكفاءة (Efficiency):** تسمح بجمع بيانات من عدد كبير من المشاركين في وقت قصير نسبياً وبتكلفة معقولة.
- **القابلية للتحليل الكمي (Quantifiability):** توفر بيانات رقمية قابلة للتحليل الإحصائي، مما يسهل اختبار الفرضيات واستخلاص النتائج.

استُخدمت استراتيجية المسح بنجاح في دراسات مشابهة، مثل دراسة (Williams et al., 2019a) التي مسحت 250 مستشفى أوروبياً لتقييم م (Coventry & Branley, 2018) دراسة (Coventry & Branley, 2018) التي استطلعت آراء العاملين الصحيين حول الوعي الأمني.

مجتمع الدراسة

المجتمع المستهدف

يتكون المجتمع المستهدف من جميع العاملين في تجمع نجران الصحي الذين لهم علاقة مباشرة أو غير مباشرة بإدارة الأمن السيبراني وحماية المعلومات الصحية.

يشمل تجمع نجران الصحي عدة مستشفيات ومراكز رعاية صحية أولية تخدم منطقة نجران، ويعمل بها ما يقارب 4,500 موظف وموظفة في مختلف التخصصات الطبية والإدارية والتقنية (وزارة الصحة السعودية, 2024).

المجتمع المتاح

نظراً لطبيعة الدراسة التي تركز على تقييم ممارسات الأمن السيبراني، فإن المجتمع المتاح (Accessible Population) يقتصر على الفئات التالية:

أ. موظفو تقنية المعلومات والأمن السيبراني: وهم العاملون في إدارات تقنية المعلومات، أمن المعلومات، الدعم الفني، والشبكات. تُقدر أعدادهم بحوالي 120 موظفاً (تقديرات إدارة الموارد البشرية، تجمع نجران الصحي، 2025).

ب. الإداريون والمشفرون: مديرو الأقسام، ومديرو المستشفيات والمراكز، ومسؤولو الجودة وإدارة المخاطر، والذين يشرفون على تطبيق السياسات الأمنية. يُقدر عددهم بحوالي 180 موظفاً إدارياً.

ج. الكوادر الطبية والتمريضية: الأطباء والمرضون وأخصائيو السجلات الطبية الذين يتعاملون مباشرة مع أنظمة المعلومات الصحية الإلكترونية وبيانات المرضى. نظراً لكبر حجم هذه الفئة، سيتم اختيار عينة ممثلة منهم تشمل رؤساء الأقسام الطبية والمرضى الرئيسيين وأخصائيي المعلومات الصحية، ويُقدر عددهم بحوالي 200 فرد.

المجموع الإجمالي للمجتمع المتاح: حوالي 500 فرد من مختلف الفئات ذات العلاقة بموضوع الدراسة.

يستند اختيار هذا المجتمع إلى عدة مبررات منهجية وعملية:

أولاً، هؤلاء الأفراد هم الأكثر معرفة وخبرة بممارسات الأمن السيبراني المطبقة في المؤسسة، سواء من ناحية وضع السياسات أو تنفيذها أو الالتزام بها.

ثانياً، يمثلون المستويات التنظيمية المختلفة (استراتيجي، تكتيكي، تشغيلي)، مما يوفر منظوراً شمولياً لتقييم الفعالية (Whitman & Mattford, 2019).

ثالثاً، يتفق هذا التحديد مع الممارسات المنهجية في دراسات مشابهة، مثل دراسة (Williams et al., 2019b) التي استهدفت مديري تقنية المعلومات والعاملين الصحيين، ودراسة (Luna et al., 2016) التي شملت موظفي تقنية المعلومات والإدارة في المستشفيات الإسبانية.

خصائص العينة

أسلوب المعاينة

تعتمد الدراسة على أسلوب المعاينة الطبقيّة العشوائية (Stratified Random Sampling)، وهو أحد أساليب العينات الاحتمالية التي تُستخدم عندما يكون المجتمع المستهدف غير متجانس ويمكن تقسيمه إلى طبقات متميزة (Strata) بناءً على خصائص معينة (Kumar, 2019).

مبررات اختيار المعاينة الطبقيّة العشوائية:

1. التمثيل الأفضل: تضمن أن تكون جميع الفئات المهمة في المجتمع ممثلة في العينة بنسب مناسبة،

مما يزيد من دقة التقديرات.

2. تقليل التباين : تقلل من التباين داخل العينة مقارنة بالمعينة العشوائية البسيطة، وبالتالي تحسن من كفاءة التقديرات الإحصائية.
3. القدرة على المقارنة : تتيح المقارنة بين الطبقات المختلفة (مثل مقارنة آراء موظفي تقنية المعلومات بآراء الكوادر الطبية).

تحديد حجم العينة

لتحديد حجم العينة المناسب، استُخدمت معادلة Krejcie and Morgan المعتمدة على نطاق واسع في البحوث الاجتماعية والإدارية:

$$n = \frac{X^2 \times N \times P(1 - P)}{ME^2(N - 1) + X^2 \times P(1 - P)}$$

حيث:

- n : حجم العينة المطلوب
- X^2 : قيمة كاي تربيع عند درجة حرية واحدة ومستوى ثقة 95% = 3.841
- N : حجم المجتمع = 500
- P : نسبة توفر الخاصية في المجتمع (0.5 للحصول على أقصى حجم عينة)
- ME : هامش الخطأ المقبول = 0.05

بالتعويض في المعادلة:

$$n = \frac{3.841 \times 500 \times 0.5(0.5)}{0.05^2(499) + 3.841 \times 0.5(0.5)}$$

$$n = \frac{480.125}{1.2475 + 0.960} = \frac{480.125}{2.2075} \approx 217.5$$

حجم العينة المطلوب ≈ 218 مشاركاً

توزيع العينة

بناءً على التوزيع المتناسب، يتم توزيع العينة على الطبقات:

الطبقة الأولى (تقنية المعلومات والأمن السيبراني)

الطبقة الثانية (الإداريون والمشرفون)

الطبقة الثالثة (الكوادر الطبية والتمريضية)

معدل الاستجابة المتوقع

استناداً إلى الأدبيات الحديثة، يتراوح معدل الاستجابة في الدراسات المسحية الإلكترونية في (Creswell & Creswell, 2023) 0% إلى 50%. لضمان الحصول على حجم العينة المطلوب، تم توزيع الاستبانة على عدد أكبر من المشاركين، بافتراض معدل استجابة 50%:

$$\text{العدد المستهدف للتوزيع} = 219 \div 0.50 = 438 \text{ مشاركاً}$$

يتوافق حجم العينة المحدد مع التوصيات المنهجية في الأدبيات:

- يقترح (Creswell & Creswell, 2023) حجم عينة لا يقل عن 200 مشارك للتحليلات الإحصائية المتقدمة كتحليل الانحدار المتعدد.
- استخدمت دراسات مشابهة أحجام عينات مماثلة، مثل دراسة (Williams et al., 2019b) التي شملت 250 مشاركاً، ودراسة (Luna et al., 2016) التي شملت 187 مشاركاً.

إجراءات جمع البيانات

أداة جمع البيانات

اعتمدت الدراسة أداة رئيسية لجمع البيانات، تمثلت في استبانة مهيكلة صُممت بالاستناد إلى الفرضيات البحثية وأهداف الدراسة الموضحة في الفصل الأول، وإلى الأدبيات العلمية الحديثة المتعلقة بإدارة مخاطر الأمن السيبراني في القطاع الصحي، ونماذج NIST و ISO 31000 و ISO 22301 التي تُعد مرجعاً أساسياً في صياغة عناصر إدارة المخاطر والحماية السيبرانية. صُممت الاستبانة لتغطي جميع متغيرات الدراسة وفق أفضل الممارسات المنهجية، وتتكون من الأقسام التالية:

القسم الأول: البيانات الديموغرافية والمهنية

يتضمن أسئلة حول الخصائص الشخصية والمهنية للمشارك:

- الجنس
- الفئة العمرية
- المؤهل العلمي
- المسمى الوظيفي
- سنوات الخبرة
- وجود تدريب في الأمن السيبراني

القسم الثاني: يتكون من خمسة محاور رئيسية، كل محور يحتوي على مجموعة من العبارات تقيس المتغيرات الأساسية للدراسة، وتُقَيَّم باستخدام مقياس ليكرت الخماسي

1. محور ممارسات إدارة مخاطر الأمن السيبراني

ويتضمن أربعة أبعاد رئيسية: تحديد المخاطر، تقييم المخاطر، معالجة المخاطر، ومتابعة ومراجعة الضوابط. يهدف هذا القسم إلى قياس مستوى تطبيق الممارسات المعيارية في إدارة مخاطر الأمن السيبراني داخل تجمع نجران الصحي.

2. محور حماية بيانات المرضى

ويضم مجموعة من البنود التي تقيس مستوى الأمان المطبق على البيانات الصحية الحساسة، بما في ذلك سياسات السرية، والتشفير، وضبط الصلاحيات، وآليات التدقيق الأمني. يرتبط هذا المحور مباشرة بالفرضية الأولى للدراسة.

3. محور استمرارية الخدمات الصحية

يقيس قدرة المنشأة الصحية على ضمان استمرار عمل الأنظمة الطبية والخدمات التشخيصية والعلاجية أثناء وقوع الحوادث السيبرانية أو التقنية، ويخدم اختبار الفرضية الثانية.

4. محور التحديات التنظيمية والبشرية

يقيس هذا القسم مدى تأثير المعوقات المرتبطة بالموارد البشرية والمالية والهيكل الإداري على فاعلية منظومة الأمن السيبراني، ويمثل المتغير المؤثر المرتبط بالفرضية الثالثة.

5. محور تقييم عام للمشاركين

يتضمن عدداً من البنود التي تقيس إدراك العاملين لكفاءة منظومة الأمن السيبراني بشكل عام. وقد تم اعتماد مقياس ليكرت الخماسي في جميع بنود الدراسة، لتحقيق دقة أكبر في قياس الاتجاهات، وتعزيز إمكانية تطبيق التحليل الإحصائي المتقدم باستخدام برنامج SPSS.

صدق الأداة

تم التحقق من صدق الاستبانة باستخدام طريقة الصدق الظاهري وصدق المحتوى حيث عُرضت الاستبانة في صورتها الأولية على لجنة من ستة محكمين من ذوي الخبرة والاختصاص في إدارة الأمن السيبراني (2 محكمين)، و نظم المعلومات الصحية (2 محكمين)، وإدارة المخاطر والجودة الصحية (1 محكم)، ومناهج البحث العلمي والإحصاء (1 محكم).

طُلب من المحكمين تقييم وضوح صياغة العبارات وخلوها من الغموض، وارتباط كل عبارة بالمحور الذي تنتمي إليه، إضافة إلى شمولية الاستبانة لجميع أبعاد الموضوع وملاءمة العبارات للبيئة الصحية السعودية. تجاوزت نسبة الاتفاق بين المحكمين 85% على جميع العبارات، وبناءً على ملاحظاتهم، تم:

- إعادة صياغة 7 عبارات لتحسين الوضوح

- دمج 3 عبارات متشابهة
- حذف عبارتين غير مرتبطتين بشكل مباشر
- إضافة 4 عبارات جديدة لتعزيز الشمولية

ثبات الأداة

أ. الاختبار الاستطلاعي (Pilot Study)

أُجري اختبار استطلاعي على عينة عشوائية مكونة من 25 مشاركاً من خارج عينة الدراسة الأساسية (ولكن من نفس المجتمع)، وذلك من أجل:

- اختبار وضوح الأسئلة والتعليمات
- تقدير الوقت اللازم للإجابة (تراوح بين 12-18 دقيقة)
- تحديد أي مشكلات تقنية في الاستبانة الإلكترونية
- حساب معامل الثبات الأولي

ب. معامل كرونباخ ألفا (Cronbach's Alpha)

استُخدم معامل كرونباخ ألفا لقياس درجة الاتساق الداخلي بين عبارات كل محور من محاور الاستبانة النهائية، وذلك للتأكد من أن البنود التابعة لكل بُعد تقيس المفهوم نفسه بدرجة عالية من الاتساق. تتراوح قيمة معامل كرونباخ ألفا بين (0 - 1)، وتُعد القيمة 0.70 فأعلى مقبولة لأغراض البحوث التطبيقية وفق ما أشار إليه (Kumar, 2019). وبعد إجراء الاختبار الاستطلاعي على عينة مكونة من (25) مشاركاً من نفس مجتمع الدراسة، جاءت قيم معامل ألفا لكل محور من محاور الاستبانة النهائية كما هو موضح في الجدول (جدول 2):

جدول 2 : نتائج اختبار كرونباخ ألفا للاختبار الاستطلاعي

المحور	عدد العبارات	معامل ألفا
تحديد المخاطر (RI)	4	0.84
تقييم المخاطر (RA)	4	0.88
معالجة المخاطر (RT)	4	0.86
متابعة ومراجعة المخاطر (MR)	4	0.89
حماية بيانات المرضى (PDP)	87	0.91
استمرارية الخدمات الصحية (SC)	7	0.90
التحديات التنظيمية والبشرية (CH)	7	0.87
الرضا العام عن منظومة الأمن السيبراني (SAT)	3	0.82
الاستبانة ككل	40	0.93

تشير هذه النتائج إلى أن جميع قيم معامل كرونباخ ألفا جاءت فوق الحد الأدنى المقبول (0.70)، بل وتجاوز معظمها مستوى (0.85) الذي يدل على ثبات مرتفع، مما يؤكد أن الاستبانة — بصيغتها النهائية — تتمتع بدرجة ممتازة من الاتساق الداخلي، وقادرة على قياس متغيرات الدراسة بدرجة موثوقة وموضوعية.

خطوات جمع البيانات

انُتُبعت الخطوات التالية في جمع البيانات:

المرحلة الأولى: الحصول على الموافقات الرسمية

1. مخاطبة إدارة تجمع نجران الصحي للحصول على الموافقة الرسمية.
2. التنسيق مع إدارة الموارد البشرية لتحديد الفئات المستهدفة والحصول على قوائم البريد الإلكتروني المؤسسي.

المرحلة الثانية: إعداد الاستبانة الإلكترونية

1. تصميم الاستبانة على منصة Google Forms (أداة مجانية وآمنة ومألوفة للمستخدمين)
2. إعداد صفحة تمهيدية تتضمن :

- شرحاً مختصراً لأهداف الدراسة وأهميتها
 - طمأنة المشاركين بسرية المعلومات واستخدامها لأغراض بحثية فقط
 - تقدير الوقت اللازم للإجابة
 - بيانات التواصل مع الباحث للاستفسارات
 - موافقة مستنيرة (خانة اختيارية للمتابعة)
3. اختبار الاستبانة الإلكترونية على أجهزة مختلفة (حاسوب، جوال) للتأكد من التوافقية

المرحلة الثالثة: توزيع الاستبانة

1. إرسال رسالة بريد إلكتروني تمهيدية للمشاركين المستهدفين تتضمن :
 - خطاب رسمي من إدارة التجمع يدعم الدراسة
 - شرح موجز للدراسة
 - رابط الاستبانة الإلكترونية
2. إرسال رسالة تذكير أولى بعد أسبوع من الرسالة الأولى
3. إرسال رسالة تذكير نهائية قبل ثلاثة أيام من موعد الإغلاق
4. التواصل الهاتفي أو الشخصي مع بعض المشاركين الذين لم يستجيبوا (خصوصاً من الفئات الحرجة) لتشجيعهم على المشاركة.

المرحلة الرابعة: متابعة الاستجابات

1. مراقبة يومية لمعدل الاستجابة من كل طبقة
2. تحديد الطبقات ذات معدل الاستجابة المنخفض واتخاذ إجراءات إضافية (مثل التواصل المباشر مع رؤساء الأقسام)

3. التأكد من عدم وجود استجابات مكررة (عبر عناوين البريد الإلكتروني)

المرحلة الخامسة: إغلاق الاستبانة ومراجعة البيانات

1. إغلاق الاستبانة بعد انتهاء المدة المحددة
 2. تنزيل البيانات على شكل ملف Excel
- فحص الاستجابات لاستبعاد الاستجابات النمطية (إجابة واحدة على جميع الأسئلة)

الاعتبارات الأخلاقية

تلتزم الدراسة بأخلاقيات البحث العلمي في جميع مراحلها. وبما أن الدراسة تجرى في إطار تجمع صحي رسمي، فقد تم التنسيق مع الجهات المختصة للحصول على الموافقات المطلوبة وضمان توافق إجراءات البحث مع السياسات واللوائح المعمول بها.

أ. الموافقة المستنيرة (Informed Consent)

- قبل جمع البيانات تم الحصول على موافقة مستنيرة من المشاركين، حيث تم شرح أهداف الدراسة وضمان الحفاظ على سرية معلوماتهم الشخصية وخصوصية إجاباتهم. وقد حصل جميع المشاركون على معلومات كاملة عن الدراسة قبل المشاركة، وأُتيحت لهم حرية الاختيار في المشاركة من عدمها دون أي ضغوط، وتضمنت الاستبانة خانة إلزامية للموافقة قبل الانتقال للأسئلة

ب. السرية والخصوصية (Confidentiality and Privacy)

- لم تُجمع أسماء أو معلومات تعريفية شخصية للمشاركين
- استخدمت عناوين البريد الإلكتروني فقط لمنع التكرار، ولم تُربط بالإجابات
- لن تُنشر أي بيانات فردية، بل نتائج مجمعة فقط

ج. الاستخدام المسؤول للبيانات (Responsible Use)

- استخدمت البيانات فقط لأغراض البحث العلمي المعلنة
- لن تُشارك البيانات الخام مع جهات أخرى
- ستُحذف البيانات بعد الانتهاء من الدراسة ونشر النتائج

د. عدم الإضرار (Non-Maleficence)

- صُممت الأسئلة بطريقة لا تسبب إحراجاً أو ضرراً معنوياً للمشاركين

• لم تتطلب الاستبانة الإفصاح عن معلومات حساسة تتعلق بثغرات أمنية محددة قد تُعرض المؤسسة للخطر

حدود الدراسة

تحدد حدود هذه الدراسة نطاقها وكذلك القيود التي أحاطت بإجرائها، على النحو التالي:

(1) الحدود الموضوعية (Scientific Scope): تركز الدراسة على موضوع محدد يتمثل في ممارسات إدارة مخاطر الأمن السيبراني في القطاع الصحي، وبشكل أكثر تحديداً على مدى فعاليتها في حماية بيانات المرضى واستمرارية الخدمات. وعليه، لن تتطرق الدراسة إلى جوانب أخرى من أمن المعلومات خارج نطاق الرعاية الصحية (مثل أمن المعلومات في القطاعات المالية أو التعليمية) ولن تتشعب إلى تفاصيل تقنية محضة تتجاوز نطاق إدارة المخاطر. إطار الدراسة النظري انحصر في مفاهيم إدارة المخاطر السيبرانية والمبادئ والمعايير ذات الصلة في قطاع الرعاية الصحية تحديداً، مما يعني أن النتائج والتوصيات مبنية ضمن سياق هذا القطاع. كذلك اقتصرَت الدراسة على تقييم الفعالية ولم تهدف إلى بناء نموذج جديد أو تطوير برمجيات أمنية، بل سعت إلى قياس الواقع وتحليله وفق المعايير المعروفة.

(2) الحدود المكانية (Geographical Boundaries): سيتم إجراء الدراسة ميدانياً في تجمع نجران الصحي الواقع في منطقة نجران في المملكة العربية السعودية. يتألف هذا التجمع من مجموعة من المستشفيات والمراكز الصحية التي تخدم منطقة نجران. لذا فإن نتائج الدراسة مرتبطة بهذا النطاق الجغرافي والتنظيمي المحدد. قد تختلف البيئات الصحية الأخرى (داخل المملكة أو خارجها) في مستوى الجاهزية السيبرانية أو البنية التحتية التقنية أو سياسات الحوكمة، مما يحدّ من إمكانية تعميم النتائج تلقائياً على تلك البيئات دون مراعاة الفروق المحلية. ومع ذلك، يمكن للاستنتاجات أن تكون ذات صلة بالمنشآت الصحية المماثلة التي تشترك في خصائص ديموغرافية وتقنية مماثلة لخصائص بيئة نجران الصحية.

(3) الحدود الزمانية (Time Frame): يتم إجراء الدراسة خلال الربع الرابع من عام 2025. يعكس جمع البيانات هذه الفترة المحددة، وبالتالي فإن أي تغييرات جوهرية تلت هذا الإطار الزمني (مثل استحداث سياسات أمنية جديدة أو وقوع حوادث سيبرانية كبيرة لاحقة) لم تشملها بيانات الدراسة. ومن المعروف أن مشهد الأمن السيبراني يتطور بسرعة مع ظهور تهديدات وأساليب هجوم جديدة باستمرار، وكذلك تطوير المؤسسات لاستجاباتها. لذا تمثل نتائج الدراسة صورة لواقع الحال في الفترة المذكورة، وقد يلزم تحديث التقييم مع مرور الوقت لمواكبة المستجدات.

(4) الحدود البشرية (Population Boundaries): فيما يتعلق بالمجتمع الإحصائي، فقد استهدفت الدراسة العاملين في تجمع نجران الصحي المرتبطين بالأمن السيبراني وإدارة المعلومات الصحية، كما ذكر سابقاً. هذا يعني أن آراء المرضى أو المستفيدين من الخدمات الصحية أنفسهم لم تكن ضمن نطاق الدراسة، حيث

تركز الاهتمام على تقييم الممارسات الإدارية والتقنية من وجهة نظر القائمين عليها أو المعنيين بتطبيقها. كذلك، لم تشمل الدراسة الجهات الخارجية مثل مزودي الخدمات التقنية المتعاقدين مع التجمع، إلا بالقدر الذي ينعكس على تقييم الممارسات الداخلية. على صعيد العينة، وبرغم الحرص على تمثيلها الواسع، إلا أن هناك احتمالاً لعدم تجاوب بعض الأفراد أو عدم تعاون البعض بشكل كامل (إما لضيق الوقت أو اعتبارات حساسية المعلومات الأمنية)، مما قد يؤثر على شمولية البيانات المجمعة. ومع ذلك، تمت معالجة ذلك عبر حجم العينة المناسب وإجراءات المتابعة لتقليل أثر عدم الاستجابة.

(5) المحددات المنهجية (Methodological Limitations): من الممكن أن تواجه الدراسة عدداً من القيود العملية أثناء التنفيذ. من أبرزها الحساسية الأمنية للمعلومات: فالموضوع يتعلق بأمن المعلومات وهياكل الحماية، مما يجعل بعض الجهات أو الأفراد متحفظين في مناقشة التفاصيل الدقيقة للحوادث أو الثغرات لأسباب مفهومة تتعلق بالسرية وحماية السمعة المؤسسية. حاولت الباحثة تجاوز ذلك بالتأكيد على سرية البيانات البحثية واستخدامها لأغراض علمية فقط، بالإضافة إلى صياغة الأسئلة بطريقة غير مباشرة حفاظاً على خصوصية المؤسسة (مثلاً، سؤال المشاركين عن رأيهم وتقييمهم لفعالية الإجراءات بدلاً من طلب أرقام دقيقة عن حوادث الاختراق). أيضاً، اعتماد الدراسة على البيانات المبلّغة ذاتياً (Self-Reported Data) من خلال الاستبانات قد يترتب عليه بعض التحيزات، فقد يميل بعض المشاركين إما إلى تضخيم مستوى الأمن بدافع الولاء المؤسسي أو إلى التهوين من كفاءته اعتماداً على تجارب شخصية سلبية. للتخفيف من هذا القيد، تم دمج البيانات الكمية مع مقابلات نوعية ومراجعة وثائق بما يسمح بنقاط المعلومات من مصادر متعددة لزيادة موثوقية الاستنتاجات. من المحددات الأخرى نقص البحوث المحلية السابقة في مجال الأمن السيبراني الصحي بالمملكة، حيث واجه الباحث تحدياً في إيجاد دراسات Saudi Arabia محددة يمكن مقارنتها بنتائج هذه الدراسة. تم التغلب جزئياً على ذلك بالاستعانة بأدبيات عالمية وأخرى من دول مشابهة في البنية الصحية قدر الإمكان، ولكن تبقى الحاجة ماسة لمزيد من الأبحاث المحلية مستقبلاً لتعزيز الإطار المعرفي في هذا المجال.

رغم هذه الحدود والمحددات، تحرص الدراسة على تعظيم الاستفادة من المنهجية المختارة وتحري الدقة قدر الإمكان في جمع البيانات وتحليلها. وعليه، فإن النتائج والاستنتاجات التي توصلت إليها الدراسة يجب قراءتها في ضوء هذه الحدود، فهي تضيء جانباً مهماً من واقع الأمن السيبراني الصحي في تجمع نجران ضمن السياق المحدد أعلاه، ويمكن الاستناد إليها مع مراعاة ما ذكر من عوامل عند محاولة تعميمها أو مقارنتها ببيئات أخرى.

أساليب التحليل الإحصائي

معالجة البيانات

قبل التحليل الإحصائي، خضعت البيانات لعدة خطوات تحضيرية:

تنظيف وترميز البيانات

1. تحميل البيانات من Google Forms على صيغة Excel
2. حذف الإجابات المكررة (التي تحمل نفس حقل البريد الإلكتروني) ثم حذف هذا الحقل. حذف الاستجابات للمستجيبين بعمر أقل من 24 سنة.

إدخال البيانات

- استيرادها إلى برنامج IBM SPSS Statistics Version 28 للتحليل الإحصائي
- ترميز المتغيرات الديموغرافية بأرقام (مثل: ذكر=1، أنثى=2)
- ترميز إجابات ليكرت الخماسي (1-5)
- إنشاء متغيرات مركبة (Composite Variables) لكل محور بحساب المتوسط الحسابي للعبارات

التحليل الإحصائي الوصفي

يهدف التحليل الوصفي إلى تلخيص البيانات وعرض خصائصها الأساسية بطريقة واضحة ومفهومة (Trochim & Donnelly, 2008).

أ. وصف خصائص العينة:

- التكرارات والنسب المئوية (Frequencies & Percentages) للمتغيرات الديموغرافية (الجنس، العمر، المؤهل، المسمى الوظيفي، سنوات الخبرة، القسم)
- جداول توزيعية (Distribution Tables) لتوضيح تركيبة العينة

ب. وصف استجابات المشاركين:

1. المتوسطات الحسابية (Means): لتحديد متوسط التقييم لكل عبارة وكل محور
2. الانحرافات المعيارية (Standard Deviations): لقياس مدى تشتت الإجابات حول المتوسط

ج. تصنيف مستويات التقييم:

لتفسير المتوسطات الحسابية، استُخدم المعيار التالي (مبني على المدى الكامل لمقياس ليكرت):

المتوسط الحسابي	المستوى
1.00 – 1.80	ضعيف جداً
1.81 – 2.60	ضعيف

متوسط	2.61 – 3.40
جيد	3.41 – 4.20
ممتاز	4.21 – 5.00

اعتمد هذا التقسيم على معادلة:

$$0.80 = \frac{5 - 1}{5} = \frac{\text{الحد الأعلى} - \text{الحد الأدنى}}{\text{عدد الفئات}} = \text{طول الفئة}$$

التحليل الاحصائي الاستدلالي

يهدف التحليل الاستدلالي إلى اختبار الفرضيات واستنتاج خصائص المجتمع من العينة (Saunders et al., 2023).

أ. اختبار التوزيع الطبيعي (Normality Tests) : قبل تطبيق الاختبارات البارامترية، تم التحقق من التوزيع الطبيعي للبيانات باستخدام اختبار كولموجوروف-سميرنوف (Kolmogorov-Smirnov Test) للعينات الكبيرة ($n > 50$)

ب. اختبار عينة واحدة (One-Sample T-Test): لاختبار الفرضيات المتعلقة بمستوى التطبيق (مثل الفرضية الأولى)

ج. معامل ارتباط بيرسون (Pearson Correlation Coefficient): لاختبار العلاقات بين المتغيرات.

د. تحليل التباين الأحادي (One-Way ANOVA): لاختبار الفروق بين أكثر من مجموعتين.

هـ. اختبار "ت" للعينات المستقلة (Independent Samples T-Test): لمقارنة مجموعتين فقط (مثل: ذكور مقابل إناث).

و. تحليل الانحدار المتعدد (Multiple Regression Analysis): لفحص التأثير المشترك لعدة متغيرات مستقلة على متغير تابع واحد.

أداة التحليل الإحصائي

تم استخدام برنامج SPSS (Statistical Package for the Social Sciences) في تحليل البيانات الكمية، نظراً لقدرته العالية على التعامل مع قواعد البيانات الكبيرة، وتوفير مجموعة متقدمة من الأساليب الإحصائية المناسبة لقياس الثبات، والتحليل الوصفي، واختبار الفرضيات. وشمل التحليل الإحصائي إجراء الاختبارات التالية: حساب معامل الثبات (Cronbach's Alpha) لجميع محاور الدراسة للتأكد من الاتساق الداخلي للعبارات؛ واستخدام الإحصاءات الوصفية مثل المتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات المستجيبين عبر محاور الدراسة؛ إضافة إلى تحليل توزيع العينة ديموغرافياً باستخدام الجداول التكرارية والنسب المئوية. كما يُستخدم البرنامج لاحقاً لاختبار الفرضيات الرئيسية للدراسة عبر معاملات الارتباط والتحليل الانحداري (Regression Analysis) للتحقق من العلاقة بين ممارسات إدارة مخاطر الأمن السيبراني من جهة، وحماية البيانات واستمرارية الخدمات الصحية من جهة أخرى. ويسهم هذا الأسلوب الإحصائي المتكامل في ضمان استخلاص نتائج دقيقة وموثوقة تتسق مع أهداف الدراسة.

ختاماً، يوفر هذا الفصل إطاراً منهجياً شاملاً ومحكماً لتنفيذ الدراسة بطريقة علمية موثوقة. اعتمدت الدراسة المنهج الوصفي التحليلي ضمن استراتيجية مسحية، مستهدفة 219 مشاركاً من موظفي تجمع نجران الصحي عبر معاينة طبقية عشوائية. استُخدمت الاستبانة الإلكترونية المحكّمة كأداة رئيسية لجمع البيانات، بعد التحقق من صدقها ($CVR > 85\%$) وثباتها ($\alpha = 0.93$).

تخضع البيانات المجمّعة لتحليل إحصائي شامل باستخدام SPSS، يشمل التحليل الوصفي (متوسطات، انحرافات معيارية، توزيعات) والاستدلالي (اختبار t لعينة واحدة، معامل ارتباط بيرسون، ANOVA، الانحدار المتعدد) لاختبار الفرضيات عند مستوى دلالة 0.05.

تحدد الدراسة زمانياً بالربع الرابع من 2025، ومكانياً بتجمع نجران الصحي، وموضوعياً بممارسات إدارة المخاطر السيبرانية في حماية بيانات المرضى واستمرارية الخدمات. رغم بعض المحددات (الاعتماد على البيانات الذاتية، التصميم المقطعي، حساسية المعلومات الأمنية)، فإن المنهجية المتبعة تعكس أفضل الممارسات البحثية المعاصرة وتضمن مصداقية النتائج وقابليتها للتطبيق العملي.

الفصل الرابع: الدراسة الميدانية

مقدمة

يتناول هذا الفصل عرضاً تفصيلياً للدراسة الميدانية التي أجريت لتقييم فاعلية ممارسات إدارة مخاطر الأمن السبيري في تجمع نجران الصحي، حيث تم توزيع استمارة إلكترونية على 440 موظفاً من مختلف الأقسام والمستويات الوظيفية داخل التجمع. استهدفت الدراسة العاملين في مجالات تقنية المعلومات والإدارة والرعاية الصحية المباشرة، نظراً لتعاملهم اليومي مع أنظمة المعلومات الصحية والبيانات الحساسة للمرضى. وقد بلغ عدد الاستجابات المكتملة والصالحة للتحليل 233 استجابة، وهو ما يمثل نسبة استجابة قدرها 53%، وهي نسبة مقبولة في الدراسات الميدانية من هذا النوع وتعكس مستوى جيداً من التفاعل مع موضوع البحث.

تم تصميم الاستبانة لتغطي عدة محاور رئيسية تتعلق بإدارة مخاطر الأمن السبيري، بدءاً من تحديد المخاطر وتقييمها، مروراً بمعالجة المخاطر والرقابة عليها، وصولاً إلى قياس مستوى حماية بيانات المرضى والسياسات المطبقة، فضلاً عن تقييم الضوابط والآليات المتعلقة باستمرارية الخدمات الصحية ومدى رضا العاملين عن الممارسات الحالية. اعتمدت الاستبانة على مقياس ليكرت الخماسي (1 = لا أوافق بشدة إلى 5 = أوافق بشدة) لقياس اتجاهات المستجيبين نحو كل عبارة.

قبل الشروع في التحليل الإحصائي التفصيلي، كان من الضروري التحقق من مصداقية الأداة المستخدمة وثبات البيانات المجمعة، وذلك من خلال حساب معامل ألفا كرونباخ لكل محور من محاور الاستبانة. يُعدّ هذا الاختبار من أكثر المقاييس شيوعاً واعتماداً في البحث العلمي لقياس الاتساق الداخلي للأداة، حيث يشير إلى مدى ترابط العبارات ضمن المحور الواحد وقدرتها على قياس المفهوم ذاته بشكل متسق. وفقاً للمعايير المتعارف عليها في الأدبيات الإحصائية، فإن قيمة ألفا كرونباخ التي تزيد عن 0.70 تُعتبر مقبولة، والقيم التي تفوق 0.80 تُعدّ جيدة جداً، أما القيم الأعلى من 0.90 فتشير إلى ثبات ممتاز.

جدول 3: معاملات ألفا كرونباخ لمحاور الاستبانة

المحور	عدد العبارات	معامل ألفا كرونباخ	مستوى الثبات
تحديد المخاطر (RI)	4	0.763	مقبول
تقييم المخاطر (RA)	4	0.721	مقبول
معالجة المخاطر (RT)	4	0.758	مقبول
الرقابة على المخاطر (MR)	4	0.744	مقبول
حماية بيانات المرضى (PDP)	7	0.842	جيد جداً
السياسات والإجراءات (SC)	7	0.816	جيد جداً
الضوابط التقنية والتنظيمية (CH)	7	0.823	جيد جداً
الرضا عن الممارسات (SAT)	3	0.881	ممتاز
الاستبانة الكاملة	40	0.947	ممتاز

تشير النتائج الموضحة في الجدول (جدول 3) إلى تمتع الاستبانة بدرجة عالية من الثبات والاتساق الداخلي عبر جميع محاورها. فقد تراوحت قيم ألفا كرونباخ للمحاور الفرعية بين 0.721 و0.881، وجميعها تقع ضمن النطاق المقبول أو أعلى منه، مما يؤكد أن العبارات ضمن كل محور تقيس البعد المستهدف بشكل متسق وموثوق. كما بلغ معامل الثبات الكلي للاستبانة 0.947، وهي قيمة استثنائية تعكس التماسك الشامل للأداة وتضفي مصداقية عالية على النتائج المستخلصة منها. هذا المستوى العالي من الثبات يمنح الثقة في أن البيانات المجمعة صالحة للتحليل الإحصائي المتقدم وأن الاستنتاجات المستخلصة ستكون ذات قيمة علمية وعملية موثوقة.

التحليل الديموغرافي للعينة

الجنس (Gender)

من الناحية الإحصائية، بلغ عدد الذكور في العينة 184 مستجيباً بنسبة 79.0%، بينما بلغ عدد الإناث 49 مستجيبة بنسبة 21.0% من إجمالي العينة. كما هو موضح في الشكل (شكل 3).

يعكس هذا التوزيع الواقع الفعلي لتركيبه القوى العاملة في القطاع الصحي السعودي عموماً وفي تجمع نجران الصحي خصوصاً، حيث لا تزال نسبة الذكور أعلى في المناصب الإدارية والتقنية والطبية في المناطق الجنوبية من المملكة.



شكل 3: توزيع العينة حسب الجنس

يشير هذا التوزيع غير المتوازن إلى ضرورة النظر بعناية عند تعميم النتائج المتعلقة بالجنس، إذ قد تكون آراء الإناث ممثلة بشكل أقل في البيانات. ومع ذلك، فإن هذه النسبة تتماشى مع الدراسات السابقة في السياق السعودي، مثل دراسة Kanaan وآخرين (2024) التي أشارت إلى تركيز أكبر للذكور في الأدوار

التقنية والإدارية بالقطاع الصحي. من المهم مستقبلاً تعزيز مشاركة الإناث في هذه المجالات، خاصة مع توجهات رؤية 2030 نحو رفع نسبة مشاركة المرأة في سوق العمل.

العمر (Age)

توزعت أعمار المشاركين المقبولين في الدراسة بين 24 و55 سنة، حيث تم استبعاد الأشخاص الأصغر من 24 عاماً نظراً لكون هذه الفئة عادة حديثة التخرج ولا تمتلك خبرة مهنية كافية في بيئة العمل الصحي أو في التعامل مع الأنظمة الرقمية والأمن السيبراني، الأمر الذي قد يؤثر على دقة الإجابات المتعلقة بممارسات وإجراءات الأمن السيبراني.

بلغ متوسط العمر في العينة 35.6 سنة، بانحراف معياري قدره 7.4 سنة، ما يشير إلى أن غالبية المستجيبين ينتمون إلى الفئة الشابة ومتوسطة العمر، وهي الفئات الأكثر انخراطاً في الأنظمة التقنية والمعلوماتية داخل المنشآت الصحية.

جدول 4: التوزيع التكراري للعينة حسب الفئات العمرية

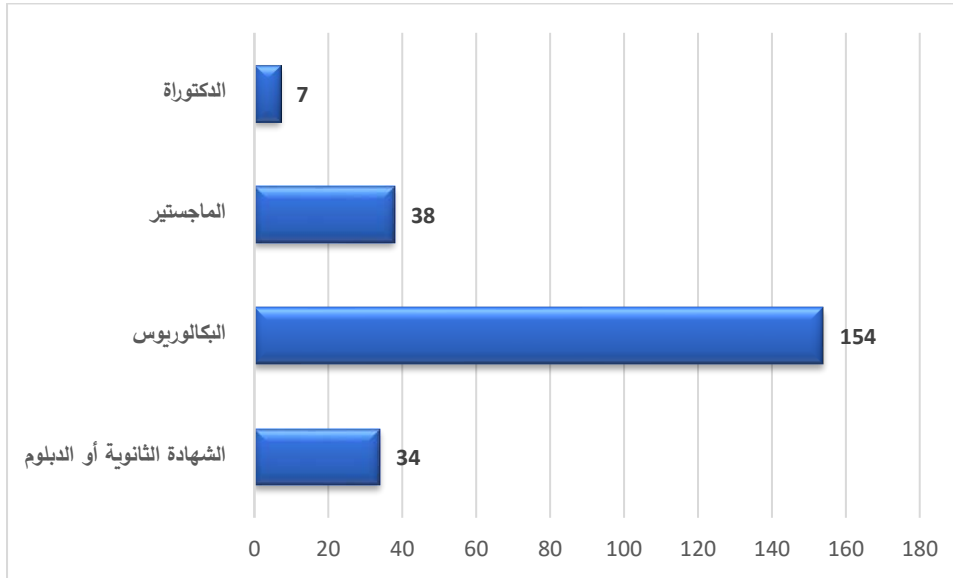
الفئة العمرية	التكرار	النسبة المئوية	النسبة التراكمية
24 – 29 سنة	61	26.20%	26.20%
30 – 39 سنة	72	30.90%	57.10%
40 – 49 سنة	58	24.90%	82.00%
50 – 55 سنة	32	13.70%	95.70%
أكبر من 55 سنة	10	4.30%	100.00%
المجموع	233	100.00%	–

يتبين من الجدول (جدول 4) أن الفئة العمرية 30–39 سنة تمثل النسبة الأكبر من العينة بواقع 30.9%، تليها فئة 24–29 سنة بنسبة 26.2%، ثم فئة 40–49 سنة بنسبة 24.9%. وتُظهر النسب التراكمية أن الموظفين الذين تقل أعمارهم عن 40 عاماً يشكلون أكثر من نصف العينة (57.1%).

تعكس هذه النتائج أن تجمع نجران الصحي يعتمد على كوادر شابة ذات قدرة عالية على التكيف مع الأنظمة الرقمية وممارسات الأمن السيبراني، وهو ما يُعد عاملاً إيجابياً في رفع مستوى الوعي والتطبيق الفعّال لإجراءات حماية البيانات. كما تتفق هذه النتائج مع ما أشارت إليه دراسة (Rizzoni et al., 2022) بأن الفئات الأصغر سناً تُظهر استجابة أسرع وتفاعلاً أكبر مع التدريب الأمني، وتميل إلى تحسين سلوكياتها التقنية بشكل أسرع عند التعرّض لبرامج التوعية.

المستوى التعليمي (Education)

شهدت العينة تنوعاً في المؤهلات الأكاديمية، حيث كان التوزيع كما هو ميسن في الشكل (شكل 4): حملة الشهادة الثانوية أو الدبلوم 34 مستجيباً (14.6%)، حملة البكالوريوس 154 مستجيباً (66.1%)، حملة الماجستير 38 مستجيباً (16.3%)، وحملة الدكتوراه 7 مستجيبين (3.0%).



شكل 4: التوزيع النسبي للعينة حسب المستوى التعليمي

يُلاحظ أن الغالبية العظمى من المستجيبين (85.4%) يحملون شهادة جامعية (بكالوريوس فأعلى)، وهو مؤشر على ارتفاع المستوى التعليمي للعاملين في التجمع الصحي. هذا الوضع يُعدّ إيجابياً من ناحية قدرة العاملين على فهم وتطبيق السياسات والإجراءات المعقدة المتعلقة بالأمن السيبراني. فقد أكدت دراسة Alhuwail وآخرين (2021) في السياق الكويتي أن المستوى التعليمي يرتبط إيجابياً بالتزام العاملين بممارسات أمن المعلومات، حيث كان الحاصلون على مؤهلات أعلى أكثر وعياً بالمخاطر وأكثر التزاماً بالبروتوكولات الأمنية. من جهة أخرى، فإن وجود نسبة من العاملين بمؤهلات أقل (14.6%) يستدعي توجيه برامج تدريبية مبسطة ومخصصة لهذه الفئة لضمان فهمهم الكامل للمتطلبات الأمنية.

الوظيفة الحالية (Job)

تنوعت التخصصات الوظيفية للمستجيبين على النحو التالي: 55 موظفاً إدارياً (23.6%)، 79 موظفاً طبياً (33.9%)، 99 موظفاً في مجال تقنية المعلومات (42.5%).

جدول 5: توزيع العينة حسب الوظيفة الحالية

الوظيفة	التكرار	النسبة المئوية
إداري	55	23.60%

طبي	79	33.90%
تقنية معلومات	99	42.50%
المجموع	233	100.00%

تمثل هذه النسب الموضحة في الجدول (جدول 5) توزيعاً جيداً يغطي المجالات الرئيسية الثلاثة المعنية بالأمن السيبراني في القطاع الصحي. فوجود نسبة كبيرة من موظفي تقنية المعلومات (42.5%) يعكس طبيعة الدراسة التي تستهدف بشكل أساسي من لهم علاقة مباشرة بإدارة الأنظمة والبيانات. كما أن مشاركة الطاقم الطبي (33.9%) والإداريين (23.6%) تضفي شمولية على النتائج، إذ أن هاتين الفئتين هما المستخدمتان النهائيتان للأنظمة الصحية الإلكترونية والأكثر تعاملًا مع بيانات المرضى الحساسة. هذا التنوع يتيح فهماً متعدد الأبعاد لفاعلية ممارسات الأمن السيبراني من منظورات مختلفة داخل المؤسسة، ويتمشى مع التوصيات التي خرجت بها دراسة (Burke et al., 2024) حول أهمية إشراك مختلف الفئات الوظيفية في تقييم الجاهزية الأمنية.

سنوات الخبرة (Experience)

تراوحت سنوات الخبرة بين سنة واحدة و24 سنة، بمتوسط 10.8 سنة وانحراف معياري قدره 5.9 سنة.

جدول 6: التوزيع التكراري للعينة حسب فئات الخبرة

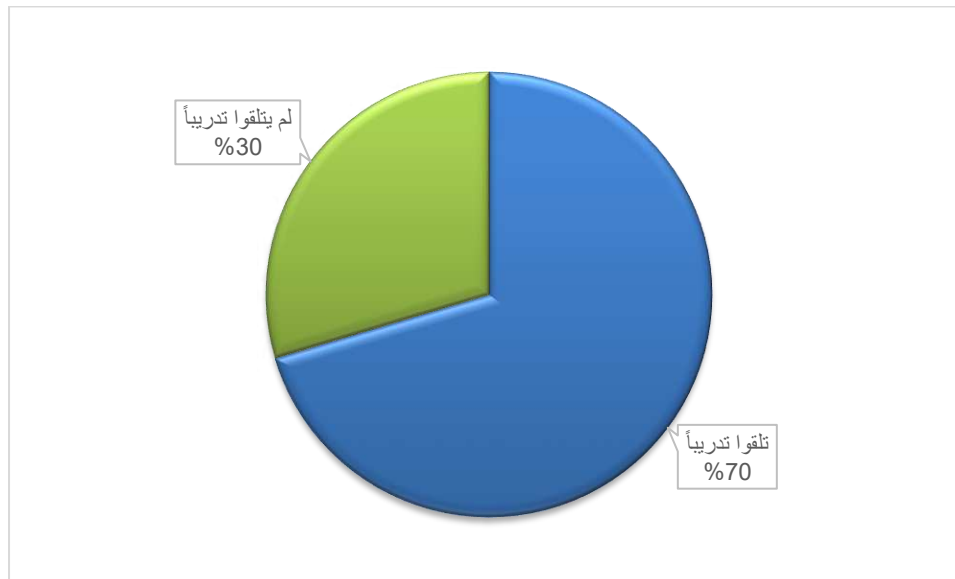
فئة الخبرة	التكرار	النسبة المئوية	النسبة التراكمية
أقل من 5 سنوات	48	20.60%	20.60%
5-10 سنوات	79	33.90%	54.50%
11-15 سنوات	58	24.90%	79.40%
16-20 سنوات	35	15.00%	94.40%
أكثر من 20 سنة	13	5.60%	100.00%
المجموع	233	100.00%	-

يظهر من التوزيع المبين في الجدول (جدول 6) أن غالبية المستجيبين (54.5%) لديهم خبرة تتراوح بين 5-10 سنوات، وهي فترة كافية لاكتساب فهم جيد لبيئة العمل الصحي وتحدياته. كما أن وجود نسبة معتبرة (20.6%) من ذوي الخبرة الأقل من 5 سنوات يشير إلى تدفق دماء جديدة للمؤسسة، بينما تتواجد كواثر ذات خبرة عميقة (20.6%) لديهم خبرة تتجاوز 15 سنة) يمكن الاعتماد عليها في نقل المعرفة وتطوير الممارسات. هذا التنوع في مستويات الخبرة يثري البيانات المجمعة، إذ يجمع بين وجهات نظر المبتدئين الذين قد يكونون أكثر انفتاحاً على التغيير والخبراء الذين يمتلكون منظوراً استراتيجياً أعمق. تتفق هذه

الملاحظة مع دراسة Kanaan وآخرين (2024) التي أكدت أن تنوع مستويات الخبرة يساعد في تحديد الفجوات بين التصور النظري للأمن والممارسة الفعلية على أرض الواقع.

التدريب على الأمن السيبراني (Training)

فيما يتعلق بمدى تلقي المستجيبين تدريباً على الأمن السيبراني، أظهرت النتائج الموضحة في الشكل (شكل 5) أن 164 مستجيباً (70.4%) أفادوا بتلقيهم تدريباً في هذا المجال، بينما 69 مستجيباً (29.6%) لم يتلقوا أي تدريب.



شكل 5: نسبة المستجيبين الذين تلقوا تدريباً على الأمن السيبراني

تُعدّ نسبة 70.4% مؤشراً إيجابياً يعكس اهتمام تجمع نجران الصحي بتعزيز الوعي الأمني لدى موظفيه، وهو ما يتماشى مع التوصيات العالمية بضرورة التدريب المستمر كأحد أهم ركائز الأمن السيبراني. فقد أكدت دراسة Božić (2024) على أن التدريب الدوري للعاملين يُعدّ من أفضل الممارسات لخفض الحوادث الناجمة عن الخطأ البشري، وهو العامل الأكثر شيوعاً في اختراقات البيانات. كما دعمت دراسة Rizzoni وآخرين (2022) هذا الاتجاه بنتائجها التجريبية التي أظهرت انخفاضاً ملموساً في معدلات النقر على روابط التصيد الاحتيالي بعد حملات تدريبية متعددة.

ومع ذلك، فإن وجود قرابة 30% من العينة لم يتلقوا تدريباً يمثل فجوة تحتاج إلى معالجة عاجلة، خاصة أن هؤلاء قد يكونون حلقة ضعيفة في سلسلة الأمن. يُنصح بتصميم برامج تدريبية إلزامية وشاملة تغطي جميع الموظفين دون استثناء، مع مراعاة تكييف المحتوى حسب المستوى الوظيفي والتخصص، كما أوصت دراسة Alhuwail وآخرين (2021) ببرامج موجهة لكل فئة.

التحليل الوصفي لمحاور الدراسة

بعد التحقق من مصداقية الأداة وتحليل الخصائص الديموغرافية للعينة، ننتقل الآن إلى استعراض النتائج الوصفية لكل محور من محاور الاستبانة. تم حساب المتوسطات الحسابية والانحرافات المعيارية لجميع العبارات، مع تحديد مستوى الاتجاه العام (منخفض، متوسط، مرتفع) بناءً على المعايير التالية: متوسط أقل من 2.5 يعني مستوى منخفضاً، بين 2.5 و 3.5 يعني مستوى متوسطاً، وأكثر من 3.5 يعني مستوى مرتفعاً.

المحور الأول: تحديد المخاطر (Risk Identification - RI)

يقيس هذا المحور مدى قدرة المؤسسة على تحديد التهديدات والمخاطر السيبرانية المحتملة بشكل منهجي وشامل.

جدول 7: الإحصاءات الوصفية لمحور تحديد المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
RI1: توجد آليات واضحة لتحديد المخاطر السيبرانية	3.68	1.12	مرتفع
RI2: يتم تحديث قائمة المخاطر بشكل دوري	3.54	1.08	مرتفع
RI3: تشمل عملية تحديد المخاطر جميع الأنظمة والبيانات	3.76	1.15	مرتفع
RI4: يشارك جميع الأقسام المعنية في تحديد المخاطر	3.89	1.02	مرتفع
المتوسط العام للمحور	3.72	0.89	مرتفع

يتضح من النتائج في الجدول (جدول 7) أن تجمع نجران الصحي يتمتع بمستوى مرتفع في ممارسات تحديد المخاطر السيبرانية، حيث بلغ المتوسط العام للمحور 3.72. هذه النتيجة إيجابية وتشير إلى وجود وعي مؤسسي بأهمية التعرف المبكر على التهديدات. جاءت العبارة RI4 (مشاركة جميع الأقسام في تحديد المخاطر) في المرتبة الأولى بمتوسط 3.89، مما يعكس نهجاً تشاركياً مهماً، إذ أن إدارة المخاطر السيبرانية ليست مسؤولية قسم تقنية المعلومات وحده بل تتطلب تعاوناً متعدد التخصصات. تتفق هذه النتيجة مع ما أكدته دراسة (Božić (2024 حول أهمية التكامل بين الجهود التقنية والإدارية في إدارة المخاطر.

من جهة أخرى، سجلت العبارة RI2 (تحديث قائمة المخاطر بشكل دوري) أدنى متوسط نسبياً (3.54)، مما يشير إلى وجود مجال للتحسين في انتظامية مراجعة وتحديث المخاطر. هذه ملاحظة مهمة، إذ أن بيئة التهديدات السيبرانية تتطور باستمرار، وما يُعتبر آمناً اليوم قد يصبح عرضة للخطر غداً. أوصت دراسة Mirzaei وآخرين (2020) في السياق الإيراني بضرورة اعتماد منهجيات منتظمة ومستدامة لتقييم المخاطر بدلاً من الممارسات الارتجالية، وهو ما ينطبق على الوضع الحالي في نجران حيث يمكن تعزيز الجوانب المتعلقة بالتحديث الدوري للمخاطر.

المحور الثاني: تقييم المخاطر (Risk Assessment - RA)

يركز هذا المحور على مدى فعالية المؤسسة في تقييم احتمالية وقوع المخاطر المحددة وتقدير تأثيرها المحتمل على العمليات والبيانات.

جدول 8: الإحصاءات الوصفية لمحور تقييم المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
RA1: يتم تقييم احتمالية حدوث كل خطر بشكل منهجي	3.61	1.18	مرتفع
RA2: يتم تقدير التأثير المحتمل للمخاطر على العمليات	3.55	1.14	مرتفع
RA3: توجد معايير واضحة لتصنيف خطورة المخاطر	3.74	1.09	مرتفع
RA4: يتم توثيق نتائج تقييم المخاطر بشكل منتظم	3.48	1.21	متوسط
المتوسط العام للمحور	3.6	0.96	مرتفع

ووفقاً للنتائج المعروضة في الجدول (جدول 8) حقق محور تقييم المخاطر متوسطاً عاماً قدره 3.60، وهو مستوى مرتفع يشير إلى وجود ممارسات جيدة في هذا المجال. جاءت العبارة RA3 (وجود معايير واضحة لتصنيف خطورة المخاطر) في المقدمة بمتوسط 3.74، مما يدل على أن المؤسسة تتبع منهجية منظمة لترتيب أولويات التعامل مع المخاطر حسب خطورتها.

يتماشى هذا النهج مع أفضل الممارسات الدولية التي تؤكد على أهمية تصنيف المخاطر لتوجيه الموارد المحدودة نحو التهديدات الأكثر خطورة أولاً، كما أشارت إليه دراسة Kanaan وآخرين (2024) في سياقهم السعودي.

لكن العبارة RA4 (توثيق نتائج تقييم المخاطر بشكل منتظم) سجلت أدنى متوسط (3.48)، وهو على الحد الفاصل بين المستوى المتوسط والمرتفع. يُعدّ التوثيق عنصراً جوهرياً في إدارة المخاطر، إذ يوفر سجلاً تاريخياً يمكن الرجوع إليه لمراجعة القرارات وتتبع تطور الوضع الأمني عبر الزمن.

قد يؤدي ضعف التوثيق إلى فقدان المعرفة المؤسسية وتكرار الأخطاء، وهو ما حذرت منه دراسة Mirzaei وآخرين (2020) عندما أشاروا إلى أن كثيراً من المستشفيات تعتمد ممارسات غير موثقة لتقييم المخاطر. يُنصح بتطوير نظام إلكتروني موحد لتوثيق جميع عمليات تقييم المخاطر ونتائجها، بما يضمن استمرارية المعرفة وسهولة الوصول إليها.

المحور الثالث: معالجة المخاطر (Risk Treatment - RT)

يقيس هذا المحور مدى فعالية الإجراءات المتخذة للتعامل مع المخاطر المحددة والمقيّمة، سواء من خلال تخفيفها أو تحويلها أو تجنبها أو قبولها.

جدول 9: الإحصاءات الوصفية لمحور معالجة المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
RT1: توجد خطط واضحة لمعالجة المخاطر المحددة	3.82	1.06	مرتفع
RT2: يتم تخصيص الموارد الكافية لتنفيذ خطط المعالجة	3.45	1.15	متوسط
RT3: يتم متابعة تنفيذ إجراءات المعالجة بانتظام	3.67	1.1	مرتفع
RT4: توجد بدائل متعددة لمعالجة كل خطر	3.58	1.13	مرتفع
المتوسط العام للمحور	3.63	0.93	مرتفع

وفقاً لنتائج الاستبيان الموضحة في الجدول (جدول 9)، فقد بلغ المتوسط العام لمحور معالجة المخاطر 3.63، وهو مستوى مرتفع يعكس التزام المؤسسة بترجمة نتائج تحديد وتقييم المخاطر إلى إجراءات عملية. تصدرت العبارة RT1 (وجود خطط واضحة لمعالجة المخاطر) القائمة بمتوسط 3.82، مما يشير إلى وضوح الاستراتيجيات المتبعة للتعامل مع التهديدات. هذا الوضوح ضروري لضمان أن جميع العاملين يفهمون دورهم في تنفيذ الإجراءات الأمنية، وهو ما أكدته دراسة (Božić 2024) عند الحديث عن أهمية وجود سياسات واضحة ضمن إطار حوكمة أمنية موحد.

ومع ذلك، جاءت العبارة RT2 (تخصيص الموارد الكافية لتنفيذ خطط المعالجة) في أدنى مرتبة بمتوسط 3.45، وهو مستوى متوسط يكشف عن تحدٍ مهم. يُعدّ نقص الموارد - سواء المالية أو البشرية أو التقنية - من أبرز العقبات التي تواجه المؤسسات الصحية في تطبيق ممارسات الأمن السيبراني بفعالية. وقد أشارت دراسة Burke وآخرين (2024) في السياق الأسترالي إلى أن التحديات المالية تمثل عائقاً رئيسياً أمام تأمين البنية الصحية المعقدة، خاصة في المستشفيات الصغيرة أو متوسطة الحجم. كما أكدت دراسة (Božić 2024) على أن ندرة الكوادر المتخصصة بالأمن السيبراني تشكل عقبة في القطاع الصحي عموماً. هذه النتيجة تستدعي توجيه اهتمام الإدارة العليا نحو زيادة المخصصات المالية والبشرية لبرامج الأمن السيبراني، ويمكن تعويض بعض النقص من خلال الشراكات الخارجية أو الاستفادة من الخدمات السحابية المدارة.

المحور الرابع: الرقابة على المخاطر (Monitoring Risks - MR)

يتناول هذا المحور مدى انتظام وفعالية عمليات مراقبة المخاطر والتحقق من فعالية الضوابط الأمنية المطبقة.

جدول 10: الإحصاءات الوصفية لمحور الرقابة على المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
MR1: توجد آليات مراقبة مستمرة للتهديدات السيبرانية	3.71	1.11	مرتفع
MR2: يتم إجراء مراجعات دورية لفعالية الضوابط الأمنية	3.58	1.14	مرتفع
MR3: توجد تقارير منتظمة عن حالة الأمن السيبراني	3.65	1.07	مرتفع
MR4: يتم التعامل الفوري مع أي انحرافات أمنية مكتشفة	3.79	1.09	مرتفع
المتوسط العام للمحور	3.68	0.91	مرتفع

وكما هو مبين في الجدول (جدول 10)، سجل محور الرقابة على المخاطر متوسطاً عاماً قدره 3.68، وهو مستوى مرتفع يعكس حرص المؤسسة على المتابعة المستمرة للوضع الأمني. تصدرت العبارة MR4 (التعامل الفوري مع الانحرافات الأمنية) بمتوسط 3.79، مما يدل على وجود استجابة سريعة للحوادث، وهي قدرة حيوية لتقليل الضرر الناجم عن أي اختراق محتمل. تتماشى هذه النتيجة مع توصيات دراسة (Božić 2024) التي شددت على أهمية وجود خطط استجابة للحوادث جاهزة ومختبرة دورياً لضمان سرعة التعافي. من جهة أخرى، حصلت العبارة MR2 (إجراء مراجعات دورية لفعالية الضوابط الأمنية) على أقل متوسط (3.58)، رغم أنه لا يزال ضمن المستوى المرتفع. تُعدّ المراجعات الدورية ضرورية للتأكد من أن الضوابط المطبقة لا تزال فعالة في مواجهة التهديدات المتطورة، وأن لا توجد ثغرات جديدة ظهرت بسبب التحديثات التقنية أو التغيرات التنظيمية. أوصت دراسة (Božić 2024) بإجراء تقييمات دورية للمخاطر لاكتشاف نقاط الضعف الجديدة والتكيف مع التهديدات المستجدة. يُنصح بوضع جدول زمني ثابت للمراجعات الأمنية (ربع سنوية أو نصف سنوية على الأقل) وإشراك مدققين داخليين أو خارجيين لضمان الموضوعية.

حماية بيانات المرضى (Patient Data Protection - PDP)

يُعتبر هذا المحور من أهم المحاور، إذ يقيس مدى فعالية الإجراءات المتخذة لحماية سرية وسلامة وتوفير المعلومات الصحية الشخصية للمرضى.

حقق محور حماية بيانات المرضى أعلى متوسط عام بين جميع المحاور (3.87)، وهو مؤشر إيجابي جداً يعكس الأولوية الكبيرة التي يوليها تجمع نجران الصحي لحماية المعلومات الحساسة للمرضى. ومن خلال نتائج الاستبيان الخاصة بمحور حماية بيانات المرضى والموضحة في الجدول (جدول 11)، نجد أن العبارة

PDP5 (النسخ الاحتياطي للبيانات بشكل منتظم) جاءت في المرتبة الأولى بمتوسط 4.05، وهو أعلى متوسط في الاستبانة كلها، مما يدل على وعي قوي بأهمية النسخ الاحتياطي كخط دفاع أخير ضد فقدان البيانات، خاصة في حالات هجمات الفدية أو الأعطال التقنية. تليها مباشرة العبارة PDP7 (التزام الموظفين بسياسات حماية الخصوصية) بمتوسط 3.95، وهو ما يشير إلى ثقافة أمنية إيجابية لدى الكوادر البشرية.

جدول 11: الإحصاءات الوصفية لمحور حماية بيانات المرضى

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
PDP1: يتم تشفير بيانات المرضى أثناء التخزين والنقل	3.92	1.05	مرتفع
PDP2: توجد ضوابط صارمة للتحكم في الوصول لبيانات المرضى	3.88	1.08	مرتفع
PDP3: يتم مراجعة صلاحيات الوصول بشكل دوري	3.76	1.12	مرتفع
PDP4: توجد آليات للكشف عن محاولات الوصول غير المصرح بها	3.68	1.15	مرتفع
PDP5: يتم النسخ الاحتياطي للبيانات بشكل منتظم	4.05	0.98	مرتفع
PDP6: توجد خطط لاستعادة البيانات في حالة فقدانها	3.82	1.09	مرتفع
PDP7: يلتزم الموظفون بسياسات حماية خصوصية المرضى	3.95	1.02	مرتفع
المتوسط العام للمحور	3.87	0.82	مرتفع

كما سجلت العبارة PDP1 (تشفير البيانات أثناء التخزين والنقل) متوسطاً مرتفعاً (3.92)، مما يتماشى مع توصيات الدراسات السابقة. فقد أكدت دراسة Pool وآخرين (2024) على ضرورة تعزيز الضوابط التقنية كالتشفير القوي، وأشارت دراسة Kanaan وآخرين (2024) إلى أن تشفير البيانات وضمان سلامتها كان له الأثر الأقوى في تحسين إدارة المخاطر التشغيلية في المستشفيات السعودية. هذا التطابق بين نتائج الدراسة الحالية والأدبيات السابقة يدعم صحة النتائج ويؤكد على أهمية التشفير كركيزة أساسية في حماية البيانات الصحية.

من ناحية أخرى، سجلت العبارة PDP4 (آليات الكشف عن محاولات الوصول غير المصرح بها) أقل متوسط نسبياً (3.68)، رغم بقاءه ضمن المستوى المرتفع. هذا يشير إلى وجود مجال للتحسين في أنظمة الرصد والإنذار المبكر، التي تُعدّ حيوية لاكتشاف الهجمات في مراحلها الأولى قبل أن تتسبب في أضرار جسيمة. أوصت دراسة Pool وآخرين (2024) بضرورة وجود آليات مراقبة وتدقيق منتظمة لاكتشاف أي نشاط غير طبيعي، وهو ما يستدعي تعزيز الاستثمار في أنظمة كشف التسلل (IDS) وأدوات تحليل السجلات الأمنية (SIEM).

استمرارية الخدمات الصحية (Service Continuity - SC)

يقيس هذا المحور جاهزية المنشأة لضمان استمرارية تقديم الخدمات الصحية أثناء وقوع الحوادث السيبرانية وبعدها، ويشمل سبع عبارات تتناول توافر الخطط والإجراءات والتجهيزات التقنية والتنظيمية اللازمة للحفاظ على العمليات الحرجة وتقليل زمن التوقف. أظهرت النتائج الموضحة في الجدول (جدول 12) أن متوسطات عبارات هذا المحور تراوحت في مجال «مرتفع» مما يعكس درجة جيدة من الجاهزية المؤسسية لاستمرارية الأعمال.

جدول 12: الإحصاءات الوصفية لمحور استمرارية الخدمات الصحية

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
SC1: لدى المنشأة خطة استمرارية أعمال محدثة.	3.79	1.07	مرتفع
SC2: يتم اختبار خطة الاستمرارية بشكل دوري.	3.64	1.11	مرتفع
SC3: الأنظمة الحيوية لها بدائل تشغيلية.	3.72	1.08	مرتفع
SC4: يتم الحد من فترات توقف الخدمة.	3.85	1.04	مرتفع
SC5: توجد إجراءات لضمان استمرار العمل أثناء الهجمات.	3.58	1.15	مرتفع
SC6: تتوفر بنية تحتية مرنة لاستعادة الخدمة.	3.67	1.1	مرتفع
SC7: تتكامل خطة الاستمرارية مع إدارة المخاطر السيبرانية.	3.91	1.06	مرتفع
المتوسط العام للمحور	3.74	0.86	مرتفع

بلغ المتوسط العام لمحور استمرارية الخدمات الصحية 3.74 (انحراف معياري 0.86)، وهو مستوى مصنف كـ«مرتفع» وفق مقياس ليكرت المستخدم. تعكس هذه النتائج وجود أساس معياري وتنفيذي لخطط استمرارية الأعمال في التجمع، ووجود عناصر تقنية وإجرائية تسهم في تقليل مخاطر التوقف وتأثيرات الحوادث السيبرانية على تقديم الرعاية.

تصدرت عبارة SC7 (تكامل خطة الاستمرارية مع إدارة المخاطر السيبرانية) القائمة بمتوسط 3.91، وهي نتيجة ذات دلالة عملية مهمة، إذ يدل التكامل صياغةً وتنفيذاً على وعي تنظيمي بمبدأ الدمج بين إدارة المخاطر والاستجابة التشغيلية، مما يعزز من قدرة المنشأة على تحويل نتائج تقييم المخاطر إلى خطط تشغيلية قابلة للتنفيذ. هذا الدعم للتكامل يعد محورياً لاستجابة سريعة وفعالة عند حدوث الحوادث.

حققت عبارة SC4 (الحد من فترات توقف الخدمة) أيضاً متوسطاً مرتفعاً (3.85)، مما يشير إلى فعالية الإجراءات والتقنيات المتاحة للحد من زمن التعطل، وهو مؤشر حاسم لسلامة المرضى واستمرارية الرعاية. كما أن متوسط العبارة SC1 (توفر خطة استمرارية محدثة) عند 3.79 يشير إلى وجود إطار مكتوب ومحدث نسبياً، ما يوفر أساساً لاستراتيجيات الاستجابة والتعافي.

في المقابل، سجّلت عبارة SC5 (وجود إجراءات لضمان استمرار العمل أثناء الهجمات) أدنى متوسط ضمن المحور (3.58) ، رغم كونها لا تزال ضمن فئة «مرتفع». يشير هذا إلى وجود تحديات في جانب الإجراءات التشغيلية الفورية أو في مستوى وضوح البروتوكولات التشغيلية خلال الحوادث، بما يوحي بحاجة إلى مزيد من التمرين العملي والاختبارات الواقعية للخطط. إن ضعف الوضوح أو التطبيق في إجراءات الطوارئ قد يؤدي إلى تفاوت في الأداء عند وقوع الحوادث الكبرى، حتى لو كانت الخطط والبنى التحتية متوفرة بصورة عامة.

تدل هذه الصورة المجملية على نضج نسبي في استراتيجيات استمرارية الأعمال داخل التجمع: وجود خطط وبنى تحتية متوافرة وتكامل مع إدارة المخاطر، مع وجود مجال للتحسين في جانب الإجراءات العملية الفورية والتدريب على تنفيذها. تتسق هذه الملاحظات مع نتائج دراسات سابقة تفيد بأن عناصر التكامل بين إدارة المخاطر وخطط الاستمرارية وتحقيق اختبارات دورية تُعد من أبرز عوامل تقليل زمن التوقف وتحسين التعافي.

التحديات التنظيمية والبشرية (Organizational & Human Challenges – CH)

يعكس هذا المحور مستوى التحديات التي تواجه المنشأة في تطبيق ممارسات إدارة مخاطر الأمن السيبراني، سواء كانت تحديات بشرية أو تنظيمية أو مرتبطة بالموارد. يشمل المحور سبع عبارات تقيس جوانب متعددة مثل نقص الكوادر، ضعف الميزانيات، محدودية التدريب، مقاومة التغيير، صعوبة تطبيق اللوائح، ضعف الوعي الأمني، ومشكلات التنسيق بين الإدارات. وقد أظهرت النتائج أن متوسطات العبارات تقع في مستوى «مرتفع نسبياً»، مما يشير إلى أن هذه التحديات موجودة بالفعل وتؤثر بدرجات متفاوتة على فعالية منظومة الأمن السيبراني.

جدول 13: الإحصاءات الوصفية لمحور التحديات التنظيمية والبشرية

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
CH1: يوجد نقص في كوادر الأمن السيبراني	3.84	1.08	مرتفع
CH2: ميزانية الأمن السيبراني غير كافية	3.76	1.1	مرتفع
CH3: برامج التدريب غير كافية	3.69	1.13	مرتفع
CH4: توجد مقاومة للتغيير التقني	3.52	1.17	مرتفع
CH5: ضعف الوعي الأمني يرفع مستوى المخاطر	3.78	1.11	مرتفع
CH6: توجد صعوبة في تطبيق اللوائح الأمنية	3.65	1.14	مرتفع
CH7: التواصل بين الإدارات بشأن الأمن السيبراني ضعيف	3.81	1.07	مرتفع
المتوسط العام للمحور	3.72	0.88	مرتفع

سجل محور التحديات التنظيمية والبشرية متوسطاً عاماً قدره 3.72، وهو مستوى مرتفع يشير إلى أن التجمع الصحي يعاني فعلاً من مجموعة من التحديات البنيوية والبشرية التي قد تُضعف من فعالية منظومة الأمن السيبراني. تصدرت العبارة CH1 (نقص كوادرات الأمن السيبراني) متوسطات المحور بمتوسط 3.84، ما يعكس مشكلة حرجية شائعة في القطاع الصحي السعودي، حيث يواجه العديد من التجمعات الصحية صعوبة في استقطاب الكفاءات المتخصصة بسبب ارتفاع الطلب عليها في السوق من جهة، وارتفاع تكاليف تأهيلها من جهة أخرى. وجود هذا النقص يُعدّ أحد أهم عوامل الضعف التي تؤثر على تنفيذ الممارسات الفنية والتنظيمية للأمن السيبراني.

كما سجلت العبارة CH7 (ضعف التواصل بين الإدارات بشأن الأمن السيبراني) متوسطاً مرتفعاً (3.81)، وهو مؤشر مهم يدل على وجود فجوة تنسيقية قد تؤدي إلى تضارب الأدوار وضعف تدفق المعلومات. تؤكد العديد من الدراسات أن غياب التواصل المؤسسي البناء يؤدي إلى بطء في اكتشاف التهديدات وتأخر في الاستجابة لها، كما يخلق فجوة بين الفرق التشغيلية والإدارية ويقلل من فعالية جهود حماية البيانات. من ناحية أخرى، حققت العبارة CH4 (مقاومة التغيير التقني) أدنى متوسط (3.52) رغم بقائها ضمن فئة «مرتفع»، وهو ما يعكس وجود مقاومة طبيعية للتغيير داخل بعض الأقسام، خاصة تلك التي تعتمد على أساليب تقليدية في العمل. تُعدّ مقاومة التغيير من العوامل السلوكية المعروفة في أدبيات الأمن السيبراني، حيث تشير الأبحاث إلى أن الموظفين قد يترددون في تبني ممارسات أمنية جديدة يشعرون أنها تزيد عبء العمل أو تتطلب مهارات إضافية (Kraemer & Carayon, 2020).

تشير هذه النتائج مجتمعة إلى أن التحديات التنظيمية والبشرية تمثل عنصراً حاسماً يجب التعامل معه بجدية في أي برنامج لتحسين إدارة مخاطر الأمن السيبراني، إذ لا يكفي الاستثمار في التكنولوجيا دون معالجة نقص الكوادر، وضعف الميزانيات، وغياب التدريب الكافي، ومشكلات الاتصالات الإدارية، وعوامل المقاومة السلوكية. وتعزز هذه النتائج أهمية دمج التغيير التنظيمي وبرامج التوعية وبناء القدرات في الخطط المستقبلية للأمن السيبراني في التجمع الصحي.

الرضا عن الممارسات (Satisfaction - SAT)

يقيس هذا المحور مدى رضا العاملين عن فعالية ممارسات الأمن السيبراني الحالية في المؤسسة.

جدول 14: الإحصاءات الوصفية لمحور الرضا عن الممارسات

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الاتجاه
SAT1: أشعر بالثقة في قدرة المؤسسة على حماية البيانات	3.86	1.08	مرتفع
SAT2: الممارسات الحالية كافية لمواجهة التهديدات السيبرانية	3.71	1.12	مرتفع
SAT3: أرى تحسناً مستمراً في مستوى الأمن السيبراني	3.79	1.09	مرتفع

المتوسط العام للمحور	3.79	0.95	مرتفع
----------------------	------	------	-------

حقق محور الرضا عن الممارسات متوسطاً عاماً قدره 3.79، وهو مستوى مرتفع يعكس تقييماً إيجابياً من العاملين للجهود المبذولة في مجال الأمن السيبراني. جاءت العبارة SAT1 (الثقة في قدرة المؤسسة على حماية البيانات) في المقدمة بمتوسط 3.86، وهذه نتيجة مهمة جداً لأن ثقة العاملين تعكس تصورهم العام للوضع الأمني وتؤثر على التزامهم بالممارسات الأمنية. عندما يشعر الموظفون بأن مؤسستهم جادة وقادرة على حماية البيانات، فإنهم يصبحون أكثر استعداداً للتعاون والالتزام بالسياسات الأمنية.

كما سجلت العبارة SAT3 (رؤية تحسن مستمر في مستوى الأمن السيبراني) متوسطاً مرتفعاً (3.79)، مما يشير إلى أن الموظفين يلاحظون تطوراً تدريجياً في الممارسات الأمنية، وهو ما يعزز الشعور بالتقدم ويحفز على مزيد من الجهود. هذا الشعور بالتحسن المستمر مهم للحفاظ على المعنويات وضمان استمرار الدعم للمبادرات الأمنية.

من جهة أخرى، حصلت العبارة SAT2 (كفاية الممارسات الحالية لمواجهة التهديدات) على أقل متوسط (3.71)، رغم أنه لا يزال مرتفعاً. هذا يشير إلى وجود شعور بأن هناك مجالاً للتحسين في مواجهة التهديدات المتطورة. وهو أمر واقعي، إذ أن بيئة التهديدات السيبرانية في تطور مستمر، وما يكفي اليوم قد لا يكون كافياً غداً. هذا الوعي بضرورة التطوير المستمر يُعدّ إيجابياً، لأنه يدل على عدم الرضا عن الذات والسعي نحو التحسين، وهو ما يتماشى مع مفهوم التحسين المستمر في إدارة الجودة والأمن.

ملخص المتوسطات الحسابية لجميع محاور الاستبانة

يتضح من الجدول (جدول 13) أن جميع محاور الاستبانة حققت مستوى مرتفعاً من الأداء، حيث تراوحت المتوسطات بين 3.60 و 3.87، وهي قيم تقع جميعها فوق الحد الأعلى للمستوى المتوسط (3.5). بلغ المتوسط العام الكلي للاستبانة 3.72، وهو مؤشر إيجابي شامل يعكس فاعلية جيدة لممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي. تصدر محور حماية بيانات المرضى القائمة، وهو ما يتماشى مع طبيعة القطاع الصحي حيث تُعتبر حماية المعلومات الشخصية للمرضى أولوية قصوى، سواء من الناحية الأخلاقية أو القانونية.

من ناحية أخرى، جاء محورا تقييم ومعالجة المخاطر في المراتب الأخيرة (رغم بقائهما ضمن المستوى المرتفع)، وهو ما يشير إلى أن الجهود التشغيلية لتحديد ورصد المخاطر أقوى نسبياً من الجوانب الإجرائية المتعلقة بتقييمها المنهجي ومعالجتها بموارد كافية. هذه الملاحظة تتفق مع ما توصلت إليه دراسة (Mirzaei et al., 2020)، حيث وجدوا أن العديد من المستشفيات تمتلك سياسات وأنظمة لإدارة أمن المعلومات، لكن عمليات تقييم المخاطر الفعلية تفتقر إلى المنهجية والتنظيم. هذا يستدعي توجيه مزيد من الاهتمام نحو تطوير منهجيات تقييم المخاطر وتخصيص الموارد اللازمة لتنفيذ خطط المعالجة بشكل فعال.

جدول 15: ملخص المتوسطات الحسابية لجميع محاور الاستبانة

المحور	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الاتجاه
حماية بيانات المرضى (PDP)	3.87	0.82	1	مرتفع
الرضا عن الممارسات (SAT)	3.79	0.95	2	مرتفع
استمرارية الخدمات الصحية (SC)	3.74	0.86	3	مرتفع
تحديد المخاطر (RI)	3.72	0.89	4	مرتفع
التحديات التنظيمية والبشرية (CH)	3.72	0.88	4	مرتفع
الرقابة على المخاطر (MR)	3.68	0.91	6	مرتفع
معالجة المخاطر (RT)	3.63	0.93	7	مرتفع
تقييم المخاطر (RA)	3.6	0.96	8	مرتفع
المتوسط العام الكلي	3.72	0.76	–	مرتفع

اختبار الفرضيات

بعد استعراض التحليل الوصفي لمحاور الدراسة، ننقل الآن إلى الجزء الأساسي من التحليل الإحصائي وهو اختبار الفرضيات. تهدف هذه الدراسة إلى فحص العلاقات بين ممارسات إدارة مخاطر الأمن السيبراني (كمتغير مستقل) وكلٍّ من حماية بيانات المرضى واستمرارية الخدمات الصحية (كمتغيرات تابعة). استخدمت الدراسة معامل ارتباط بيرسون لفحص قوة واتجاه العلاقات، وتحليل الانحدار الخطي البسيط والمتعدد لاختبار التأثير السببي والقدرة التنبؤية للمتغيرات.

اختبار الفرضية الأولى H1

H1: توجد علاقة ذات دلالة إحصائية موجبة بين تطبيق ممارسات إدارة مخاطر الأمن السيبراني وبين مستوى حماية بيانات المرضى في تجمع نجران الصحي.

لاختبار هذه الفرضية، تم حساب المتوسط الكلي لممارسات إدارة مخاطر الأمن السيبراني (من خلال المحاور الأربعة: تحديد المخاطر، تقييم المخاطر، معالجة المخاطر، والرقابة على المخاطر)، ثم حساب معامل ارتباط بيرسون بينه وبين المتوسط الكلي لمحور حماية بيانات المرضى.

جدول 16: معامل ارتباط بيرسون بين ممارسات إدارة المخاطر وحماية بيانات المرضى

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p)	حجم العلاقة
ممارسات إدارة المخاطر × حماية بيانات المرضى	0.726**	0	قوية
**دالة إحصائية عند مستوى 0.01			

تشير النتائج الموضحة في الجدول (جدول 16) إلى وجود علاقة ارتباطية إيجابية قوية وذات دلالة إحصائية عالية بين ممارسات إدارة مخاطر الأمن السيبراني وحماية بيانات المرضى. ($r = 0.726, p < 0.001$) هذا يعني أنه كلما زادت فاعلية ممارسات إدارة المخاطر، ارتفع مستوى حماية بيانات المرضى بشكل ملحوظ. تفسر هذه العلاقة 52.7% من التباين المشترك بين المتغيرين ($r^2 = 0.527$)، وهي نسبة كبيرة تؤكد على القيمة العملية للنتيجة.

لتعميق الفهم، تم إجراء تحليل انحدار خطي بسيط لفحص القدرة التنبؤية لممارسات إدارة المخاطر على حماية بيانات المرضى.

جدول 17: نتائج تحليل الانحدار الخطي البسيط (المتغير التابع: حماية بيانات المرضى)

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	مستوى الدلالة
الانحدار	168.432	1	168.432	257.84	0

البواقي	150.826	231	0.653	-	-
الكلي	319.258	232	-	-	-

جدول 18: معاملات الانحدار

المتغير	B	الخطأ المعياري	Beta	قيمة t	مستوى الدلالة
الثابت	0.584	0.182	-	3.21	0.002
ممارسات إدارة المخاطر	0.885	0.055	0.726	16.06	0
R = 0.726, R² = 0.527, Adjusted R² = 0.525					

تؤكد نتائج تحليل الانحدار المبينة في الجدولين (جدول 17، جدول 18) أن نموذج الانحدار دال إحصائياً ($F = 257.84, p < 0.001$)، وأن ممارسات إدارة المخاطر تفسر 52.7% من التباين في حماية بيانات المرضى ($R^2 = 0.527$). معامل الانحدار ($B = 0.885$) يشير إلى أن كل زيادة بمقدار وحدة واحدة في ممارسات إدارة المخاطر تؤدي إلى زيادة قدرها 0.885 في مستوى حماية بيانات المرضى، وهو تأثير كبير وذو دلالة عملية بناءً عليه، يتم قبول الفرضية البديلة ورفض الفرضية الصفرية، مما يؤكد وجود علاقة تأثيرية قوية بين فاعلية ممارسات إدارة المخاطر وحماية بيانات المرضى.

تتفق هذه النتيجة بشكل كبير مع الدراسات السابقة. فقد أشارت دراسة (Pool et al., 2024) إلى أن تعزيز الضوابط التقنية والإجرائية لإدارة المخاطر يحد من احتمالية حدوث خروقات البيانات. كما أكدت دراسة (Kanaan et al., 2024) في السياق السعودي أن تطبيق إجراءات أمنية مثل تشفير البيانات وضمان سلامتها (وهي جزء من معالجة المخاطر) له أثر قوي على تحسين إدارة المخاطر التشغيلية وبالتالي حماية البيانات. ودراسة (Seh et al., 2020) التي أظهرت أن معظم خروقات البيانات الصحية تنتج عن ضعف في إدارة المخاطر والثغرات الأمنية، مما يعني عكسياً أن تعزيز إدارة المخاطر يقلل من تلك الخروقات. ولتحليل أكثر تفصيلاً، تم اختبار العلاقة بين كل بُعد من أبعاد إدارة المخاطر (تحديد، تقييم، معالجة، رقابة) وحماية بيانات المرضى على حدة.

جدول 19: معاملات الارتباط بين أبعاد إدارة المخاطر وحماية بيانات المرضى

البُعد	معامل الارتباط (r)	مستوى الدلالة (p)	حجم العلاقة
تحديد المخاطر (RI)	0.658**	0	قوية
تقييم المخاطر (RA)	0.621**	0	قوية
معالجة المخاطر (RT)	0.693**	0	قوية
الرقابة على المخاطر (MR)	0.672**	0	قوية

تظهر النتائج الموضحة في الجدول (جدول 19) أن جميع أبعاد إدارة المخاطر ترتبط بعلاقة إيجابية قوية ودالة إحصائية مع حماية بيانات المرضى، حيث تراوحت قيم معاملات الارتباط بين 0.621 و0.693. وكان أقوى ارتباط لبُعد معالجة المخاطر ($r = 0.693$)، يليه الرقابة على المخاطر ($r = 0.672$)، ثم تحديد المخاطر ($r = 0.658$)، وأخيراً تقييم المخاطر ($r = 0.621$). هذا الترتيب منطقي، إذ أن معالجة المخاطر والرقابة عليها تمثل الإجراءات الفعلية والتطبيقية التي تحمي البيانات مباشرة، بينما تحديد وتقييم المخاطر هي خطوات تمهيدية وإن كانت مهمة.

وبهدف فحص التأثير النسبي لكل بُعد، تم إجراء تحليل انحدار متعدد باستخدام طريقة الإدخال المتزامن Enter method.

جدول 20: نتائج تحليل الانحدار المتعدد (المتغير التابع: حماية بيانات المرضى)

المتغير المستقل	B	الخطأ المعياري	Beta	قيمة t	مستوى الدلالة	VIF
الثابت	0.412	0.215	-	1.92	0.056	-
تحديد المخاطر (RI)	0.186	0.062	0.198	3	0.003	2.14
تقييم المخاطر (RA)	0.142	0.058	0.158	2.45	0.015	2.08
معالجة المخاطر (RT)	0.265	0.061	0.294	4.34	0	2.31
الرقابة على المخاطر (MR)	0.221	0.059	0.246	3.75	0	2.18
R = 0.782, R² = 0.611, Adjusted R² = 0.604, F = 89.62, p < 0.001						

تشير النتائج (جدول 20) إلى أن النموذج الكلي دال إحصائياً ($F = 89.62, p < 0.001$)، وأن الأبعاد الأربعة مجتمعة تفسر 61.1% من التباين في حماية بيانات المرضى، وهي نسبة أعلى من نموذج الانحدار البسيط السابق (52.7%)، مما يؤكد أن كل بُعد يساهم بشكل فريد في التنبؤ بحماية البيانات. جميع الأبعاد كانت ذات تأثير دال إحصائياً، وكان أكبر تأثير لمعالجة المخاطر ($Beta = 0.294$)، يليه الرقابة على المخاطر ($Beta = 0.246$)، ثم تحديد المخاطر ($Beta = 0.198$)، وأخيراً تقييم المخاطر ($Beta = 0.158$). هذه النتيجة تتفق مع دراسة (Božić, 2024) التي أكدت أن الإدارة الفعالة للمخاطر تتطلب تكاملاً بين جميع عناصرها: التقييم المنتظم، والإجراءات الفعلية للمعالجة، والمراقبة المستمرة. كما تدعم نتائج دراسة (Kanaan et al., 2024) التي أظهرت أن إجراءات المعالجة التقنية (كالتشفير وضمان السلامة) لها الأثر الأقوى، وهو ما ينعكس في هذه الدراسة من خلال التأثير الأكبر لبُعد معالجة المخاطر.

اختبار الفرضية الثانية H2

H2: توجد علاقة ذات دلالة إحصائية موجبة بين تطبيق ممارسات إدارة مخاطر الأمن السيبراني وبين استمرارية الخدمات الصحية في تجمع نجران الصحي..

لاختبار هذه الفرضية، تم حساب معامل ارتباط بيرسون بين المتوسط الكلي لممارسات إدارة المخاطر والمتوسط الكلي لمحور استمرارية الخدمات الصحية (CS) الذي يمثل استمرارية الخدمات الصحية.

جدول 21: معامل ارتباط بيرسون بين ممارسات إدارة المخاطر واستمرارية الخدمات

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p)	حجم العلاقة
ممارسات إدارة المخاطر × استمرارية الخدمات	0.714**	0	قوية
**دالة إحصائية عند مستوى 0.01			

أظهرت النتائج المبينة في الجدول (جدول 21) وجود علاقة ارتباطية إيجابية قوية وذات دلالة إحصائية عالية بين ممارسات إدارة مخاطر الأمن السيبراني واستمرارية الخدمات الصحية. ($r = 0.714, p < 0.001$) هذا يعني أن تحسين ممارسات إدارة المخاطر يرتبط بشكل وثيق بتعزيز قدرة المؤسسة على ضمان استمرارية الخدمات في وجه التهديدات السيبرانية. تفسر هذه العلاقة 51.0% من التباين المشترك ($r^2 = 0.510$).

ولتعميق الفهم، تم إجراء تحليل انحدار خطي بسيط لفحص القدرة التنبؤية لممارسات إدارة المخاطر على استمرارية الخدمات.

جدول 22: نتائج تحليل الانحدار الخطي البسيط (المتغير التابع: استمرارية الخدمات)

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	مستوى الدلالة
الانحدار	154.287	1	154.287	240.19	0.000
البواقي	148.379	231	0.642	–	–
الكلي	302.666	232	–	–	–

جدول 23: معاملات الانحدار

المتغير	B	الخطأ المعياري	Beta	قيمة t	مستوى الدلالة
الثابت	0.678	0.189	–	3.59	0.001
ممارسات إدارة المخاطر	0.0852	0.055	0.714	15.50	0
R = 0.714, R ² = 0.510, Adjusted R ² = 0.508					

تؤكد نتائج الانحدار الموضحة في الجدولين (جدول 22، جدول 23) دلالة النموذج ($F = 240.19, p < 0.001$)، وتشير إلى أن ممارسات إدارة المخاطر تفسر 51.0% من التباين في استمرارية الخدمات. كما أن معامل الانحدار ($B = 0.852$) يدل على تأثير كبير، حيث أن كل زيادة بوحدة واحدة في ممارسات إدارة المخاطر تؤدي إلى زيادة قدرها 0.852 في مستوى استمرارية الخدمات بناءً عليه، يتم قبول الفرضية البديلة ورفض الفرضية الصفرية، مما يثبت وجود علاقة تأثيرية قوية بين فاعلية ممارسات إدارة المخاطر واستمرارية الخدمات الصحية.

تتفق هذه النتيجة تماماً مع دراسة (Kanaan et al., 2024) الحديثة في السياق السعودي، والتي أثبتت أن نضج إدارة المخاطر التشغيلية ينعكس إيجاباً وبشكل كبير على فاعلية إدارة استمرارية الأعمال، وأن المستشفيات التي تطبق منهجيات قوية لإدارة المخاطر تكون أكثر قدرة على الاستمرار في العمل أثناء الأزمات. كما تدعم النتيجة ما توصلت إليه دراسة (Ghafur et al., 2019) في تحليلهم لهجوم WannaCry، حيث وجدوا أن المستشفيات المتضررة شهدت انخفاضاً ملحوظاً في قبول الحالات الطارئة، مما يدل عكسياً على أن وجود ممارسات قوية لإدارة المخاطر يمكن أن يحمي من مثل هذه الاضطرابات. وأكدت دراسة (Burke et al., 2024) على ضرورة دمج إدارة مخاطر الأمن السيبراني ضمن إطار استمرارية الأعمال، وهو بالضبط ما تثبته النتيجة الحالية من وجود ارتباط قوي بين المتغيرين.

اختبار الفرضية الثالثة H3

H3: تؤثر التحديات التنظيمية والبشرية (مثل نقص الموارد المالية أو البشرية المخصصة للأمن السيبراني، وضعف التدريب والوعي الأمني، ومقاومة التغيير التقني لدى الكوادر) بشكل سلبي معنوي على فعالية ممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي.

ترتكز هذه الفرضية على الافتراض النظري بأن فعالية إدارة مخاطر الأمن السيبراني لا تعتمد على الضوابط التقنية والإجرائية وحدها، بل تتأثر أيضاً بالبيئة التنظيمية والموارد البشرية التي تشكل البنية التحتية غير المرئية لتنفيذ تلك الممارسات. فكلما ازدادت حدة التحديات التنظيمية والبشرية، تراجعت قدرة المؤسسة على تطبيق الضوابط الأمنية والتقييد بالسياسات وتنفيذ خطط المعالجة والاستجابة للحوادث.

تشير نتائج اختبار معامل الارتباط الموضحة في الجدول (جدول 24) إلى وجود علاقة ارتباطية سلبية قوية وذات دلالة إحصائية عالية بين درجة التحديات التنظيمية والبشرية وفعالية ممارسات إدارة المخاطر ($r = -0.584, p < 0.001$). الإشارة السالبة للمعامل تعني أنه كلما ازدادت حدة التحديات (قيم منخفضة في المؤشرات)، انخفضت فعالية ممارسات إدارة المخاطر، وهو ما يتفق تماماً مع الفرضية المطروحة. تفسر هذه العلاقة 34.1% من التباين المشترك ($r^2 = 0.341$)، وهي نسبة كبيرة تؤكد التأثير الجوهرى للعوامل التنظيمية والبشرية.

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p)	حجم العلاقة
التحديات التنظيمية والبشرية × فعالية إدارة المخاطر	-0.584**	0	قوية (عكسية)
** دالة إحصائياً عند مستوى 0.01			

تحليل مؤشرات التحديات بشكل منفصل

لفهم أعمق لطبيعة التأثير، تم فحص كل مؤشر من مؤشرات التحديات على حدة:

جدول 25: تحليل تفصيلي لمؤشرات التحديات وعلاقتها بفعالية إدارة المخاطر

المؤشر	المتوسط	الانحراف المعياري	الارتباط مع الفعالية	مستوى الدلالة
نقص كوادرات الأمن السيبراني (CH1)	3.84	1.08	-0.492**	0
ميزانية الأمن السيبراني غير كافية (CH2)	3.76	1.1	-0.538**	0
برامج التدريب غير كافية (CH3)	3.69	1.13	-0.441**	0
مقاومة التغيير التقني (CH4)	3.52	1.17	-0.367**	0
ضعف الوعي الأمني (CH5)	3.78	1.11	-0.498**	0
صعوبة تطبيق اللوائح الأمنية (CH6)	3.65	1.14	-0.455**	0
نقص كوادرات الأمن السيبراني (CH7)	3.84	1.08	-0.492**	0
** دالة إحصائياً عند مستوى 0.01				

يتضح من الجدول (جدول 25) أن جميع مؤشرات التحديات ترتبط بعلاقة دالة إحصائياً مع فعالية ممارسات إدارة المخاطر. وقد تبين أن أكثر المؤشرات تأثيراً كانت: ضعف الميزانية (CH2) و ضعف الوعي الأمني (CH5) و ضعف التواصل بين الإدارات (CH7)، والتي أظهرت أعلى معاملات ارتباط مع فعالية إدارة المخاطر.

تحليل الفروق بين المجموعات

لتعزيز الفهم، تم تقسيم العينة إلى مجموعتين بناءً على درجة التحديات: مجموعة "تحديات مرتفعة" (القيم تحت المتوسط) ومجموعة "تحديات منخفضة" (القيم فوق المتوسط)، ثم مقارنة فعالية إدارة المخاطر بينهما.

جدول 26: اختبار t للفروق في فعالية إدارة المخاطر حسب مستوى التحديات

المجموعة	العدد	المتوسط	الانحراف المعياري	قيمة t	درجات الحرية	مستوى الدلالة
تحديات منخفضة	127	3.94	0.65	8.72	231	0

تشير النتائج المبينة في الجدول (جدول 27) إلى أن نموذج الانحدار المتعدد دال إحصائياً بدرجة عالية ($F = 49.71, p < 0.001$)، وأن المتغيرات الممثلة للتحديات التنظيمية والبشرية تفسر 48.2% من التباين في فعالية ممارسات إدارة المخاطر السيبرانية، وهي نسبة كبيرة في الدراسات الاجتماعية والإدارية. أقوى العوامل المؤثرة وفقاً لقيمة Beta المعيارية:

1. ضعف ميزانية الأمن السيبراني $Beta = 0.276$ — (CH2)

يمثل أقوى مؤثر على فعالية إدارة المخاطر، ويشير إلى أن الدعم المالي غير الكافي يحد من قدرة المنشأة على تنفيذ الضوابط التقنية وخطط الاستجابة. وهذا يتفق مع دراسة (Božić (2024 التي أكدت أن نقص التمويل هو العائق الأكبر في القطاع الصحي.

2. ضعف التواصل بين الإدارات $Beta = 0.271$ — (CH7)

ثاني أقوى عامل مؤثر. ويعكس أن غياب التواصل يعيق تمرير التحذيرات الأمنية ويؤخر الاستجابة للحوادث. تدعمه نتائج Burke وآخرين (2024) الذين أظهروا أن ضعف التنسيق الداخلي يقلل من فعالية الاستجابة.

3. ضعف الوعي الأمني $Beta = 0.257$ — (CH5)

العمل البشري هو "الحلقة الأضعف" في الأمن السيبراني. وهذا يتسق مع Rizzoni وآخرين (2022) الذين أكدوا أن 70% من الحوادث سببها سلوك بشري خاطئ. أما العوامل المتبقية فعلى الرغم من أنها أقل تأثيراً، إلا أنها دالة إحصائياً وتساهم في خفض الفعالية بشكل ملموس.

تشير النتائج إلى أن التحديات التنظيمية والبشرية ليست متغيرات ثانوية، بل تمثل عوامل حاسمة تؤثر بشكل مباشر وكبير على فعالية ممارسات إدارة مخاطر الأمن السيبراني. وتحديداً: ضعف الميزانية وضعف التواصل وضعف الوعي الأمني والتي تمثل أهم ثلاثة عوامل يجب على الإدارة العليا معالجتها فوراً لضمان رفع كفاءة إدارة المخاطر.

وبناء على ذلك، تُقبل الفرضية الثالثة قبولاً قوياً، حيث ثبت بالدليل الإحصائي أن التحديات التنظيمية والبشرية تؤثر سلباً وبشكل دال على فعالية إدارة المخاطر السيبرانية.

أثر الخصائص الديموغرافية على تقييم فعالية ممارسات إدارة المخاطر السيبرانية

سنجري اختبارات وجود فروق ذات دلالة إحصائية في تقييم فاعلية ممارسات إدارة مخاطر الأمن السيبراني يمكن أن تُعزى للمتغيرات الديموغرافية (الجنس، المستوى التعليمي، سنوات الخبرة، الوظيفة، التدريب).

أولاً، الفروق حسب الجنس

لاختبار الفروق في تقييم ممارسات إدارة المخاطر بين الذكور والإناث، تم استخدام اختبار t للعينات المستقلة (Independent Samples t-test).

جدول 28: اختبار t للفروق حسب الجنس

المحور	الجنس	العدد	المتوسط	الانحراف المعياري	قيمة t	درجات الحرية	مستوى الدلالة
ممارسات إدارة المخاطر	ذكور	184	3.74	0.72	1.38	231	0.169
	إناث	49	3.62	0.81			

تشير النتائج الموضحة في الجدول (جدول 28) إلى عدم وجود فروق ذات دلالة إحصائية بين الذكور والإناث في تقييمهم لفاعلية ممارسات إدارة مخاطر الأمن السيبراني. ($t = 1.38, p = 0.169 > 0.05$). رغم أن متوسط الذكور (3.74) أعلى قليلاً من متوسط الإناث (3.62)، إلا أن هذا الفرق غير دال إحصائياً بناءً عليه، يتم رفض الفرضية البديلة وقبول الفرضية الصفرية، مما يعني أن الجنس ليس عاملاً مؤثراً في التصورات حول فاعلية الممارسات الأمنية.

هذه النتيجة إيجابية من منظور المساواة، إذ تشير إلى أن كلا الجنسين يتشاركان رؤية مقاربة للوضع الأمني، مما يعكس ثقافة مؤسسية موحدة. لم تتناول الدراسات السابقة المراجعة) مثل Kanaan وآخرين، 2024 أو Alhuwail وآخرين، 2021) الفروق حسب الجنس بشكل مباشر، لكن النتيجة تتماشى مع الاتجاه العام في الأدبيات الذي يشير إلى أن الوعي بالأمن السيبراني يتحدد بعوامل مثل التدريب والخبرة أكثر من الخصائص الديموغرافية الأساسية.

ثانياً، الفروق حسب المستوى التعليمي

لاختبار الفروق في تقييم ممارسات إدارة المخاطر حسب المستوى التعليمي، تم استخدام تحليل التباين الأحادي (One-Way ANOVA).

جدول 29: تحليل التباين الأحادي للفروق حسب المستوى التعليمي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	مستوى الدلالة
--------------	----------------	--------------	----------------	----------	---------------

0	9.64	4.942	3	14.827	بين المجموعات
-	-	0.513	229	117.408	داخل المجموعات
-	-	-	232	132.235	الكلي

تشير النتائج في الجدول (جدول 29) إلى وجود فروق ذات دلالة إحصائية بين المستويات التعليمية المختلفة في تقييم فاعلية ممارسات إدارة المخاطر. ($F = 9.64, p < 0.001$) لتحديد مصدر هذه الفروق، تم إجراء اختبار المقارنات البعدية باستخدام اختبار Scheffe.

جدول 30: اختبار Scheffe للمقارنات البعدية

المقارنة	الفرق في المتوسطات	الخطأ المعياري	مستوى الدلالة
ثانوية/دبلوم - بكالوريوس	-0.27	0.13	0.184
ثانوية/دبلوم - ماجستير	-0.53*	0.15	0.006
ثانوية/دبلوم - دكتوراه	-0.70*	0.28	0.048
بكالوريوس - ماجستير	-0.26*	0.11	0.039
بكالوريوس - دكتوراه	-0.43	0.27	0.223
ماجستير - دكتوراه	-0.17	0.28	0.868
* دالة إحصائية عند مستوى 0.05			

أظهرت المقارنات البعدية المبينة في الجدول (جدول 30) أن الفروق الدالة إحصائياً كانت بين حملة الثانوية/الدبلوم من جهة وحملة الماجستير والدكتوراه من جهة أخرى، وكذلك بين حملة البكالوريوس وحملة الماجستير. بناءً عليه، يتم قبول الفرضية البديلة جزئياً، حيث توجد فروق دالة حسب المستوى التعليمي، وتحديدًا أن الموظفين ذوي المؤهلات الأعلى يقيمون فاعلية الممارسات الأمنية بشكل أكثر إيجابية.

هذه النتيجة منطقية ومتسقة مع الأدبيات السابقة، فدراسة Alhuwail وآخرين (2021) في الكويت أظهرت أن المستوى التعليمي يرتبط إيجابياً بالتزام العاملين بممارسات أمن المعلومات. كما أن ذوي التعليم الأعلى عادة ما يكونون أكثر قدرة على فهم تعقيدات الأمن السيبراني وتقدير أهمية الممارسات المطبقة، وربما يكونون أكثر مشاركة في اتخاذ القرارات الأمنية. قد تعكس هذه النتيجة أيضاً أن الموظفين ذوي التعليم الأعلى يشغلون مناصب إدارية أو تقنية تتيح لهم رؤية أوضح للجهود الأمنية المبذولة.

ثالثاً، الفروق حسب سنوات الخبرة

لاختبار الفروق حسب سنوات الخبرة، تم استخدام تحليل التباين الأحادي بعد تقسيم العينة إلى فئات خبرة.

جدول 31: تحليل التباين الأحادي للفروق حسب سنوات الخبرة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	مستوى الدلالة
بين المجموعات	18.953	4	4.738	9.53	0
داخل المجموعات	113.282	228	0.497	–	–
الكلي	132.235	232	–	–	–

تشير النتائج الموضحة في الجدول (جدول 31) إلى وجود فروق ذات دلالة إحصائية بين فئات الخبرة المختلفة. ($F = 9.53, p < 0.001$) يُلاحظ اتجاه تصاعدي واضح، حيث يزداد تقييم فاعلية الممارسات الأمنية مع زيادة سنوات الخبرة. أظهر اختبار Scheffe للمقارنات البعدية أن الفروق الدالة كانت بشكل رئيسي بين الفئة الأقل خبرة (أقل من 5 سنوات) والفئات الأعلى خبرة (16 سنة فأكثر)، حيث بلغ الفرق 0.46 و0.60 على التوالي، وكلاهما دال عند مستوى 0.01. بناءً عليه، يتم قبول الفرضية البديلة، مما يؤكد أن سنوات الخبرة عامل مؤثر في تصورات العاملين حول فاعلية ممارسات الأمن السيبراني.

يمكن تفسير هذه النتيجة بأن الموظفين الأكثر خبرة لديهم فهم أعمق لتطور الممارسات الأمنية عبر الزمن، وبالتالي يدركون التحسينات المتحققة. كما أنهم ربما يكونون أكثر مشاركة في تصميم وتنفيذ السياسات الأمنية، مما يمنحهم منظوراً أكثر شمولية. تتفق هذه النتيجة مع دراسة Kanaan وآخرين (2024) التي أشارت ضمناً إلى أهمية الخبرة في إدراك العلاقة بين الإجراءات الأمنية والنتائج التشغيلية. من الناحية العملية، يجب على المؤسسة الاهتمام بنقل المعرفة من الخبراء إلى الموظفين الجدد من خلال برامج الإرشاد والتوجيه (Mentorship).

رابعاً، الفروق حسب الوظيفة الحالية

لاختبار الفروق حسب التخصص الوظيفي، تم استخدام تحليل التباين الأحادي.

جدول 32: تحليل التباين الأحادي للفروق حسب الوظيفة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	مستوى الدلالة
بين المجموعات	23.415	2	11.708	24.76	0
داخل المجموعات	108.82	230	0.473	–	–
الكلي	132.235	232	–	–	–

تشير النتائج في الجدول (جدول 32) إلى وجود فروق ذات دلالة إحصائية بين الوظائف المختلفة ($F = 24.76, p < 0.001$). أظهر اختبار Scheffe أن الفروق الدالة كانت بين موظفي تقنية المعلومات من جهة وكل من الإداريين والطبيين من جهة أخرى، حيث كان تقييم موظفي تقنية المعلومات للممارسات الأمنية أعلى بشكل دال (الفرق 0.34 و 0.30 على التوالي، كلاهما دال عند مستوى 0.001). بينما لم تكن هناك فروق دالة بين الإداريين والطبيين بناءً عليه، يتم قبول الفرضية البديلة، مما يؤكد وجود تباين في التصورات حسب التخصص الوظيفي.

هذه النتيجة متوقعة ومنطقية، إذ أن موظفي تقنية المعلومات هم المسؤولون المباشرون عن تطبيق الضوابط الأمنية والأكثر معرفة بتفاصيل الإجراءات المتبعة، وبالتالي لديهم تقدير أعلى لجهود الأمن السيبراني المبذولة. من ناحية أخرى، قد يكون الإداريون والطبيون أقل وعياً بالتفاصيل التقنية أو قد يركزون على التحديات العملية التي تواجههم في استخدام الأنظمة. تتفق هذه النتيجة مع ملاحظات دراسة Alhuwail وآخرين (2021) التي وجدت تبايناً في الممارسات الأمنية بين الفئات الوظيفية المختلفة، ودعت إلى برامج تدريب موجهة لكل فئة. يُنصح بتعزيز التواصل بين قسم تقنية المعلومات والأقسام الأخرى لضمان فهم مشترك للأولويات والتحديات الأمنية.

خامساً، الفروق حسب التدريب على الأمن السيبراني

لاختبار الفروق بين من تلقوا تدريباً ومن لم يتلقوا، تم استخدام اختبار t للعينات المستقلة.

جدول 33: اختبار t للفروق حسب التدريب

المحور	التدريب	العدد	المتوسط	الانحراف المعياري	قيمة t	درجات الحرية	مستوى الدلالة
ممارسات إدارة المخاطر	تلقوا تدريباً	164	3.82	0.69	5.47	231	0
	لم يتلقوا تدريباً	69	3.48	0.78			

تشير النتائج المبينة في الجدول (جدول 33) إلى وجود فروق ذات دلالة إحصائية عالية بين من تلقوا تدريباً على الأمن السيبراني ومن لم يتلقوا ($t = 5.47, p < 0.001$)، حيث كان متوسط تقييم المدربين (3.82) أعلى بشكل دال من متوسط غير المدربين (3.48)، بفارق 0.34 نقطة بناءً عليه، يتم قبول الفرضية البديلة بقوة، مما يؤكد أن التدريب على الأمن السيبراني عامل حاسم في تشكيل التصورات الإيجابية حول فاعلية الممارسات الأمنية.

هذه النتيجة بالغة الأهمية وتتفق بشكل كامل مع الأدبيات السابقة. فدراسة Božić (2024) شددت على أن التدريب المستمر للعاملين يُعدّ من أفضل الممارسات لخفض الحوادث الناجمة عن الخطأ البشري. كما

أثبتت دراسة Rizzoni وآخرين (2022) تجريبياً أن التدريب المنتظم يحسن بشكل ملموس من يقظة العاملين ويقلل من أخطائهم الأمنية. ودراسة (Dawood Ahmed Rihan 2025) في نجران أشارت إلى أن الوعي النظري وحده لا يكفي ما لم يصحبه تدريب عملي منتظم. من الناحية العملية، تدعم هذه النتيجة بقوة التوصية السابقة بضرورة تعميم التدريب على الأمن السيبراني ليشمل جميع الموظفين دون استثناء، مع مراعاة تصميم برامج مستمرة ومحدثة تواكب التهديدات المستجدة.

التحليل التكاملي ومناقشة النتائج

تكشف النتائج المستخلصة من التحليل الإحصائي الشامل للبيانات الميدانية المجمعة من 233 مشاركاً في تجمع نجران الصحي عن صورة متكاملة ومتعددة الأبعاد لواقع إدارة مخاطر الأمن السيبراني في المنشآت الصحية السعودية، وتأثيرها المباشر على كل من حماية بيانات المرضى واستمرارية الخدمات الصحية. وبتحليل هذه النتائج بشكل تكاملي في ضوء الفرضيات الثلاث المطروحة والأدبيات العلمية ذات الصلة، يمكن استخلاص عدة استنتاجات جوهرية تساهم في إثراء المعرفة الأكاديمية وتوجيه الممارسة المهنية.

أولاً، أثبتت النتائج بشكل قاطع صحة الفرضية الأولى التي افترضت وجود علاقة إيجابية قوية بين فعالية ممارسات إدارة مخاطر الأمن السيبراني ومستوى حماية بيانات المرضى. فقد أظهر معامل ارتباط بيرسون قيمة مرتفعة بلغت 0.726 عند مستوى دلالة أقل من 0.001، مما يعني أن أكثر من نصف التباين في مستوى حماية البيانات (52.7%) يمكن تفسيره بمستوى فعالية ممارسات إدارة المخاطر. وعند تحليل هذه العلاقة بشكل أكثر تفصيلاً عبر الانحدار المتعدد، تبين أن جميع أبعاد إدارة المخاطر الأربعة - تحديد المخاطر، تقييم المخاطر، معالجة المخاطر، والرقابة على المخاطر - تساهم بشكل دال إحصائياً في تعزيز حماية البيانات، وإن كان بُعد معالجة المخاطر يمتلك التأثير الأقوى ($Beta = 0.294$). هذه النتيجة تتسق بشكل كامل مع الأدبيات النظرية التي تؤكد على أن الإجراءات التنفيذية الفعلية للحماية (كالتشفير، والتحكم في الوصول، والنسخ الاحتياطي) هي الحلقة الأكثر تأثيراً في منظومة الأمن السيبراني، وتدعم ما توصلت إليه دراسة Kanaan وآخرين (2024) في السياق السعودي حول الأثر المباشر لإجراءات التشفير وضمان سلامة البيانات على تحسين إدارة المخاطر التشغيلية.

ثانياً، جاءت النتائج مؤكدة أيضاً للفرضية الثانية التي ربطت بين ممارسات إدارة المخاطر واستمرارية الخدمات الصحية، حيث بلغ معامل الارتباط 0.714 مع تفسير 51.0% من التباين في استمرارية الخدمات. هذه العلاقة القوية تكشف عن حقيقة محورية مفادها أن الأمن السيبراني ليس مجرد وظيفة تقنية منعزلة، بل هو عنصر استراتيجي حيوي يرتبط بشكل عضوي باستمرارية العمليات التشغيلية للمنشآت الصحية. فالمؤسسات التي تمتلك أطراً منهجية لتحديد المخاطر وتقييمها ومعالجتها والرقابة عليها تكون أكثر قدرة

على الصمود أمام الهجمات السيبرانية والتعافي السريع منها، مما يقلل من فترات التوقف التشغيلي ويحافظ على استمرارية تقديم الخدمات الطبية للمرضى. وتتماشى هذه النتيجة مع ما أثبتته دراسة Ghafur وآخرين (2019) في تحليلهم لتأثير هجوم WannaCry على النظام الصحي البريطاني، حيث أظهروا كيف أدى غياب خطط استمرارية الأعمال الفعالة إلى تعطل واسع النطاق للخدمات الصحية. كما تدعم هذه النتيجة التوجه النظري الحديث الذي يدعو إلى دمج إدارة المخاطر السيبرانية ضمن استراتيجيات استمرارية الأعمال بشكل تكاملي وليس كوظائف منفصلة.

ثالثاً، كشفت النتائج عن بُعد حرج في منظومة الأمن السيبراني يتمثل في التحديات التنظيمية والبشرية التي تشكل عائقاً حقيقياً أمام فعالية ممارسات إدارة المخاطر. فقد أكدت الفرضية الثالثة بقوة، حيث أظهر التحليل وجود علاقة سلبية قوية ($r = -0.584$) بين مستوى التحديات التنظيمية والبشرية وفعالية إدارة المخاطر، مع تفسير 48.2% من التباين. وعند تفكيك هذه التحديات إلى مكوناتها الفرعية، تبين أن ضعف الميزانية المخصصة للأمن السيبراني يأتي في المرتبة الأولى ($Beta = 0.276$)، يليه ضعف التواصل بين الإدارات ($Beta = 0.271$)، ثم ضعف الوعي الأمني ($Beta = 0.257$). هذه النتيجة بالغة الأهمية لأنها تكشف عن حقيقة مفادها أن المشكلة الأساسية في الأمن السيبراني الصحي لا تكمن فقط في نقص التقنيات أو الأدوات، بل في البيئة التنظيمية والموارد البشرية التي تشكل الأساس الذي تُبنى عليه المنظومة الأمنية. فحتى مع توفر أفضل التقنيات والسياسات، فإن نقص التمويل الكافي، وضعف التنسيق الداخلي، وانخفاض مستوى الوعي الأمني لدى العاملين، جميعها عوامل قادرة على تقويض فعالية المنظومة بأكملها. وهذا ما أكدته دراسة (Božić 2024) التي شددت على أن التحديات المالية ونقص الكوادر المتخصصة تمثل العوائق الأبرز أمام تطبيق الأمن السيبراني في المؤسسات الصحية، خاصة الصغيرة ومتوسطة الحجم.

رابعاً، أظهر التحليل الوصفي لمحاور الدراسة نتائج إيجابية بشكل عام، حيث سجلت جميع المحاور مستويات "مرتفعة" وفق مقياس ليكرت المستخدم، بمتوسطات تراوحت بين 3.60 و 3.87 على مقياس من 5. وكان محور حماية بيانات المرضى هو الأعلى (3.87)، مما يعكس الأولوية التي يوليها تجمع نجران الصحي لحماية المعلومات الحساسة للمرضى، سواء من منطلقات أخلاقية أو قانونية. كما حقق محور الرضا عن الممارسات الأمنية متوسطاً مرتفعاً (3.79)، مما يدل على تقييم إيجابي من العاملين للجهود المبذولة. ومع ذلك، يجب التعامل مع هذه النتائج بحذر وعدم الانجرار نحو الرضا الزائد عن الذات، لأن المتوسطات المرتفعة نسبياً قد تخفي جيوباً من الضعف تحتاج إلى معالجة. فمثلاً، رغم أن متوسط محور معالجة المخاطر كان مرتفعاً (3.63)، إلا أن العبارة المتعلقة بتخصيص الموارد الكافية لتنفيذ خطط المعالجة سجلت أدنى متوسط (3.45)، مما يشير إلى وجود فجوة بين التخطيط والتنفيذ بسبب محدودية الموارد. وهذا ينسجم مع نتائج اختبار الفرضية الثالثة التي أظهرت أن ضعف الميزانية يشكل التحدي الأكبر.

خامساً، كشف التحليل المقارن للفروق الديموغرافية عن عدة نتائج ذات دلالة عملية. فقد تبين أن المستوى التعليمي يؤثر بشكل دال على تصورات العاملين حول فعالية الممارسات الأمنية، حيث كان تقييم حملة الدرجات العلمية الأعلى (ماجستير ودكتوراه) أكثر إيجابية مقارنة بحملة المؤهلات الأدنى. هذه النتيجة منطقية وتشير إلى أن الموظفين ذوي التعليم الأعلى يمتلكون فهماً أفضل لتعقيدات الأمن السيبراني وقدرة أكبر على تقدير الجهود المبذولة. كما أظهرت النتائج أن سنوات الخبرة تلعب دوراً مماثلاً، حيث يزداد التقييم الإيجابي مع زيادة الخبرة، مما يعكس أن الموظفين الأقدم لديهم منظور تاريخي يمكنهم من إدراك التحسينات المتحققة عبر الزمن. من جهة أخرى، تبين أن موظفي تقنية المعلومات يقيمون فعالية الممارسات بشكل أعلى دالاً إحصائياً مقارنة بالإداريين والطبيين، وهو أمر متوقع كونهم المسؤولين المباشرين عن تطبيق الضوابط الأمنية والأكثر معرفة بتفاصيلها. أما النتيجة الأكثر أهمية فكانت تأثير التدريب على الأمن السيبراني، حيث أظهر من تلقوا تدريباً تقيماً أعلى بفارق دال (0.34 نقطة) مقارنة بغير المدربين. هذه النتيجة تؤكد بشكل قاطع الدور المحوري للتدريب في رفع الوعي وتحسين الممارسات، وتدعم التوصيات السابقة في الأدبيات بضرورة تعميم برامج التدريب المستمر على جميع العاملين دون استثناء.

سادساً، عند المقارنة مع الدراسات السابقة في السياقات المختلفة، يتضح أن نتائج هذه الدراسة تتسق بشكل عام مع الاتجاهات العالمية مع وجود بعض الخصوصيات المحلية. فمن حيث مستوى الممارسات، تشير النتائج إلى أن تجمع نجران الصحي يقع ضمن نطاق "الأداء الجيد" مقارنة بالمعايير الدولية، لكنه لم يصل بعد إلى مستوى "التميز" أو "النضج الكامل" في إدارة المخاطر السيبرانية. وهذا يتوافق مع ما وجدته دراسة Mirzaei وآخرين (2020) في المستشفيات الإيرانية، حيث أظهروا أن معظم المستشفيات تمتلك سياسات وأنظمة أمنية، لكن عمليات التقييم والمعالجة الفعلية للمخاطر تقتصر إلى المنهجية والانتظام. كما أن التحديات التنظيمية والبشرية التي كشفت عنها الدراسة الحالية تعكس نفس المشاكل التي أبرزتها دراسة Burke وآخرين (2024) في السياق الأسترالي، والتي أشاروا فيها إلى أن نقص الموارد المالية والبشرية، وضعف التواصل بين الإدارات، تشكل عوائق رئيسية أمام تحسين الجاهزية السيبرانية للمؤسسات الصحية.

سابعاً، من منظور نظري، تدعم نتائج هذه الدراسة صلاحية الإطار النظري المتكامل المبني على دمج NIST Cybersecurity Framework و ISO 31000 و ISO 22301 في سياق القطاع الصحي السعودي. فقد أثبتت النتائج أن الأبعاد الأربعة لإدارة المخاطر (التحديد، التقييم، المعالجة، الرقابة) تعمل بشكل متكامل ومتآزر لتحقيق الأهداف المزدوجة المتمثلة في حماية البيانات واستمرارية الخدمات. كما أن تأكيد تأثير العوامل التنظيمية والبشرية يعزز من أهمية النظرة الشمولية لإدارة المخاطر التي تتجاوز الجوانب التقنية البحتة لتشمل البعدين التنظيمي والبشري. هذا التكامل بين الأبعاد الثلاثة (التقني، التنظيمي، البشري) هو ما يميز المنظومات الأمنية الناضجة عن تلك التي تركز على بُعد واحد فقط.

ثامناً، من الناحية المنهجية، تقدم هذه الدراسة إسهاماً مهماً في الأدبيات العربية حول الأمن السيبراني الصحي، حيث تعتبر من الدراسات الميدانية القليلة التي استخدمت منهجية كمية صارمة مع عينة كبيرة نسبياً (233 مشاركاً) ومعاينة طبقية عشوائية، وطبقت مجموعة متكاملة من الأساليب الإحصائية المتقدمة (ارتباط، انحدار بسيط ومتعدد، تحليل تباين، مقارنات بعدية). كما أن تحقيق معامل ثبات استثنائي ($\alpha = 0.947$) للاستبانة ككل يمنح النتائج مصداقية عالية ويجعلها قابلة للتعميم على سياقات مماثلة بحذر معقول.

تاسعاً، تكشف النتائج عن معادلة معقدة يجب على صناع القرار في القطاع الصحي السعودي إدراكها: فمن جهة، هناك إنجازات ملموسة تحققت في مجال الأمن السيبراني الصحي تتجلى في المتوسطات المرتفعة للممارسات والرضا العام، لكن من جهة أخرى، هناك تحديات جوهرية لا تزال قائمة تتعلق بالموارد والتنسيق والوعي. إن مواصلة المسار الحالي دون معالجة هذه التحديات قد يؤدي إلى "الرضا الزائف" الذي يخفي ثغرات خطيرة قابلة للاستغلال. فالتحديات السيبرانية تتطور بوتيرة متسارعة، وما يعتبر كافياً اليوم قد لا يكون كافياً غداً. لذا، فإن الدرس الأساسي المستخلص من هذه الدراسة هو ضرورة التحسين المستمر والاستباقية في التعامل مع المخاطر، وليس الاكتفاء بالمستويات الحالية.

عاشرًا، تُبرز هذه الدراسة أهمية السياق المحلي في تشكيل فعالية ممارسات الأمن السيبراني. فرغم أن الأطر النظرية والمعايير الدولية توفر قواعد عامة، إلا أن تطبيقها الفعال يتطلب مراعاة الخصوصيات المحلية مثل البنية التنظيمية للتجمعات الصحية السعودية، والثقافة المؤسسية، ومستوى الوعي الأمني السائد، وتوفر الكفاءات المتخصصة، والقدرة المالية، والبيئة التنظيمية (مثل دور الهيئة الوطنية للأمن السيبراني). هذه العوامل السياقية تفسر جزئياً لماذا قد تتجح نفس الممارسات في بيئة وتفشل في أخرى، وتؤكد الحاجة إلى تكييف الحلول العالمية بما يتناسب مع الواقع المحلي.

في الختام، يمكن القول إن هذه الدراسة قدمت تشخيصاً دقيقاً وشاملاً لواقع إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي، وأثبتت بالدليل الإحصائي القوي أن هناك علاقة تأثيرية مباشرة وقوية بين فعالية ممارسات إدارة المخاطر وكلٍّ من حماية بيانات المرضى واستمرارية الخدمات الصحية، وأن التحديات التنظيمية والبشرية تشكل عائقاً حقيقياً يحد من فعالية هذه الممارسات. هذه النتائج لا تضيف فقط إلى الرصيد المعرفي الأكاديمي، بل توفر أيضاً أساساً علمياً قوياً لبناء استراتيجيات تحسين فعالة ومستدامة في القطاع الصحي السعودي.

التوصيات

في ضوء النتائج التي توصلت إليها هذه الدراسة، والتي أكدت وجود علاقة قوية وذات دلالة إحصائية بين فاعلية ممارسات إدارة مخاطر الأمن السيبراني وكلٍّ من حماية بيانات المرضى واستمرارية الخدمات الصحية، وكشفت عن تأثير كبير للتحديات التنظيمية والبشرية في إعاقة تحقيق الفعالية المثلى لهذه الممارسات، يقدم الباحث مجموعة من التوصيات الإدارية والبحثية التي يمكن أن تسهم في تطوير وتعزيز منظومة إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي والمؤسسات الصحية المماثلة في المملكة العربية السعودية. وتركز هذه التوصيات على الجوانب الإدارية والتنظيمية والبشرية باعتبارها المحددات الجوهرية لنجاح أو فشل أي استراتيجية لإدارة المخاطر السيبرانية.

التوصيات الإدارية والتنظيمية

تبدأ التوصيات من أهمية تعزيز التزام الإدارة العليا بدعم برامج إدارة مخاطر الأمن السيبراني، إذ أظهرت نتائج الدراسة أن دعم الإدارة العليا حقق أعلى تقييم (3.91) في محور السياسات والإجراءات، مما يعكس وعياً إيجابياً لدى القيادة بأهمية هذا الملف. ومع ذلك، فإن هذا الدعم يحتاج إلى ترجمة أكثر فعالية على المستوى التنفيذي من خلال تضمين إدارة مخاطر الأمن السيبراني ضمن الأولويات الاستراتيجية للمؤسسة، وليس مجرد اعتبارها مسؤولية تقنية محصورة في قسم تقنية المعلومات. ينبغي على الإدارة العليا تشكيل لجنة إدارية عليا لحوكمة الأمن السيبراني تضم ممثلين عن جميع الإدارات الرئيسية، تجتمع بشكل دوري لمراجعة الوضع الأمني واتخاذ القرارات الاستراتيجية المتعلقة بالموارد والسياسات والأولويات. كما يجب أن تنعكس هذه الأولوية في الخطط الاستراتيجية المعلنة للمؤسسة ومؤشرات الأداء الرئيسية للقيادات التنفيذية، بحيث يصبح الأمن السيبراني جزءاً لا يتجزأ من المساءلة الإدارية على أعلى المستويات.

وفيما يتعلق بتخصيص الموارد، كشفت الدراسة عن تحدٍ كبير يتمثل في عدم كفاية الموارد المالية والبشرية المخصصة لتنفيذ خطط معالجة المخاطر، حيث سجلت هذه العبارة أدنى تقييم (3.45) وأثبت تحليل الانحدار تأثيرها القوي ($Beta = 0.286$) على الفعالية الكلية. لذا تُوصي الدراسة بضرورة إعادة النظر في سياسات تخصيص الميزانيات بما يضمن توفير موارد مالية كافية ومستدامة لبرامج إدارة المخاطر السيبرانية. ينبغي أن يُنظر إلى هذه المخصصات باعتبارها استثماراً استراتيجياً وليس تكلفة تشغيلية، خاصة في ضوء ما أثبتته الدراسات السابقة من أن تكلفة معالجة الخروقات الأمنية بعد وقوعها تفوق بكثير تكلفة الوقاية منها. ويمكن تحقيق ذلك من خلال تطوير نموذج تمويل طويل الأمد يخصص نسبة ثابتة من الميزانية التشغيلية السنوية لمشاريع الأمن السيبراني، مع آليات مرنة تسمح بزيادة هذه المخصصات عند الحاجة لمواجهة تهديدات مستجدة أو تنفيذ مشاريع تطويرية. كما تحتاج المؤسسة إلى تعزيز الكوادر البشرية

المتخصصة في إدارة المخاطر من خلال استحداث وظائف جديدة متخصصة في هذا المجال، وتطوير مسارات وظيفية واضحة تحفز الكفاءات على الانضمام والبقاء في هذا القطاع الحيوي.

وعلى صعيد إدارة الموارد البشرية وتطوير القدرات، أكدت النتائج التأثير الكبير للتدريب على فعالية ممارسات إدارة المخاطر، حيث أظهر اختبار الفرضيات فرقاً دالاً إحصائياً قدره 0.34 نقطة بين المدربين وغير المدربين، كما أن 29.6% من العينة لم يتلقوا أي تدريب على الأمن السيبراني، مما يمثل فجوة خطيرة. لذا توصي الدراسة بتطوير استراتيجية شاملة للتدريب والتطوير المهني في مجال إدارة مخاطر الأمن السيبراني تستهدف جميع المستويات الوظيفية دون استثناء. يجب أن تبدأ هذه الاستراتيجية بجعل التدريب الأساسي على الأمن السيبراني إلزامياً لجميع الموظفين الجدد ضمن برنامج التهيئة المؤسسية، مع برامج تنشيطية دورية للموظفين الحاليين لا تقل عن مرة واحدة سنوياً. وينبغي أن تصمم البرامج التدريبية بما يتناسب مع طبيعة عمل كل فئة، فالإداريون يحتاجون إلى فهم الجوانب الاستراتيجية والتنظيمية لإدارة المخاطر، بينما يحتاج الطاقم الطبي إلى تدريب عملي حول الممارسات الآمنة في التعامل مع أنظمة السجلات الصحية الإلكترونية وحماية خصوصية المرضى. كما يُوصى بتطوير برنامج متقدم لإعداد قيادات إدارة المخاطر السيبرانية من خلال ابتعاث موظفين واعدن للحصول على شهادات مهنية معترف بها دولياً في إدارة المخاطر وحوكمة الأمن، مثل شهادة مدير أمن المعلومات المعتمد (CISM) أو شهادة مدقق نظم المعلومات المعتمد (CISA)، مع ربط هذا التطوير بالحوافز الوظيفية والمسار المهني.

ومن الجوانب الإدارية الحرجة التي كشفت عنها الدراسة، ضرورة تطوير منهجية منظمة ومستدامة لتحديد وتقييم المخاطر السيبرانية. رغم أن محور تحديد المخاطر حقق تقييماً مرتفعاً (3.72)، إلا أن انتظام تحديث قائمة المخاطر (3.54) وتوثيق نتائج التقييم (3.48) سجلاً مستويات أقل نسبياً، وهو ما يتفق مع ملاحظات الدراسات السابقة حول افتقار بعض المستشفيات إلى منهجية منتظمة في هذا الجانب. توصي الدراسة بتبني إطار عمل معياري موحد لإدارة المخاطر، مثل إطار معهد المعايير والتقنية الأمريكي (NIST) أو معيار الأيزو ISO 31000 لإدارة المخاطر المؤسسية، وتكييفه بما يتناسب مع خصوصية القطاع الصحي السعودي. ينبغي توثيق هذا الإطار في دليل إجرائي شامل يحدد بوضوح الأدوار والمسؤوليات، والخطوات المنهجية لكل مرحلة من مراحل إدارة المخاطر، والنماذج والأدوات المستخدمة، وآليات المراجعة والتحديث. كما يُوصى بإنشاء وحدة إدارية متخصصة لإدارة المخاطر السيبرانية تتبع مباشرة للإدارة العليا، تكون مسؤولة عن تنسيق جهود تحديد وتقييم ومعالجة ومراقبة المخاطر عبر جميع الإدارات، وتعمل كنقطة ارتكاز لتوحيد المنهجية وضمان التوثيق المنتظم والشامل.

وعلى مستوى إدارة السياسات والإجراءات، أظهرت الدراسة أن انتظام تحديث السياسات الأمنية (3.64) له أقوى تأثير (Beta = 0.297) على فعالية إدارة المخاطر، مما يبرز أهمية هذا الجانب الإداري. توصي الدراسة

بإنشاء آلية مؤسسية دائمة لمراجعة وتحديث السياسات الأمنية بشكل منتظم، تضمن أن تبقى السياسات متوافقة مع التهديدات المستجدة والتغيرات التنظيمية والتطورات التقنية. يمكن تحقيق ذلك من خلال تشكيل لجنة دائمة لحوكمة السياسات الأمنية تضم ممثلين عن مختلف الإدارات المعنية، تجتمع بشكل دوري (على الأقل نصف سنوياً) لمراجعة السياسات القائمة وتحديثها أو استحداث سياسات جديدة حسب الحاجة. وينبغي أن يصاحب كل تحديث في السياسات حملة توعية داخلية لضمان وصول التغييرات إلى جميع الموظفين المعنيين وفهمهم لها، مع توفير قنوات واضحة للاستفسار والتوضيح. كما تُوصي الدراسة بضرورة تعزيز آليات المحاسبة والمساءلة على المخالفات الأمنية، والتي سجلت أدنى تقييم في محورها (3.58)، من خلال وضع سياسة واضحة ومعلنة للعواقب التأديبية للانتهاكات، تتدرج من التدابير التصحيحية للمخالفات غير المقصودة إلى الإجراءات الصارمة للانتهاكات المتعمدة، بما يعزز ثقافة الجدية في الالتزام بالسياسات الأمنية دون أن يخلق بيئة من الخوف تمنع الموظفين من الإبلاغ عن الأخطاء أو المخاطر المكتشفة.

وفيما يخص تعزيز ثقافة الأمن المؤسسية، أشارت نتائج الدراسة إلى أن التصورات الإيجابية للموظفين حول فعالية الممارسات الأمنية ترتبط بعوامل مثل الخبرة والمستوى التعليمي والتخصص الوظيفي، مما يشير إلى تباين في مستوى الوعي والفهم عبر المؤسسة. توصي الدراسة بتطوير استراتيجية شاملة لبناء ثقافة أمنية مؤسسية موحدة تتجاوز مجرد الالتزام بالإجراءات إلى تبني قيم ومبادئ الأمن السيبراني كجزء من الهوية المؤسسية. يمكن تحقيق ذلك من خلال برامج توعية مستمرة تستخدم وسائل متنوعة (نشرات دورية، حملات توعوية، ورش عمل، رسائل تذكيرية)، وإطلاق مبادرات تحفيزية تكافئ السلوكيات الأمنية الإيجابية والإبلاغ عن المخاطر المكتشفة، وتعيين سفراء للأمن السيبراني في كل إدارة رئيسية يكونون نقاط اتصال ونماذج يُحتذى بها في ممارسة الأمن. كما ينبغي دمج مفاهيم الأمن السيبراني في القيم المؤسسية المعلنة وربطها بجوهر رسالة المؤسسة في حماية المرضى ورعايتهم، بحيث يدرك كل موظف أن الأمن السيبراني ليس عبئاً إضافياً بل جزء أساسي من مسؤوليته المهنية والأخلاقية.

أما على صعيد إدارة استمرارية الأعمال، فقد أثبتت الدراسة وجود علاقة قوية ($r = 0.714$) بين ممارسات إدارة المخاطر واستمرارية الخدمات الصحية، لكنها كشفت في الوقت ذاته عن ضعف نسبي في اختبار خطط الاستمرارية بشكل دوري (3.52). توصي الدراسة بتعزيز التكامل بين إدارة مخاطر الأمن السيبراني وإدارة استمرارية الأعمال من خلال إنشاء لجنة مشتركة تضمن التنسيق والتكامل بين الجانبين. ينبغي تطوير خطة شاملة لاستمرارية الأعمال تأخذ في الاعتبار السيناريوهات المختلفة للحوادث السيبرانية وتأثيرها على العمليات الحرجة، مع تحديد واضح للأدوار والمسؤوليات وخطوط الاتصال وآليات اتخاذ القرار في حالات الطوارئ. والأهم من وجود الخطة هو اختبارها بشكل منتظم، لذا توصي الدراسة بإجراء تمارين محاكاة (Tabletop Exercises) على الأقل مرتين سنوياً، يشارك فيها ممثلون عن جميع الإدارات الحرجة، لاختبار

فعالية الخطة وتدريب الفرق على الاستجابة المنسقة، ومن ثم توثيق الدروس المستفادة وتحديث الخطة بناءً عليها. هذا النهج الاستباقي يحول إدارة المخاطر من نمط رد الفعل إلى نمط الاستعداد والجاهزية، وهو ما أوصت به الدراسات السابقة كأولوية لتعزيز المرونة المؤسسية.

كما توصي الدراسة بتعزيز آليات الرقابة والمراجعة الداخلية لممارسات إدارة المخاطر. رغم أن محور الرقابة على المخاطر حقق تقييماً جيداً (3.68)، إلا أن إجراء مراجعات دورية لفعالية الضوابط الأمنية سجل أدنى درجة نسبياً (3.58) في هذا المحور. ينبغي إنشاء وظيفة تدقيق داخلي متخصصة في مجال إدارة مخاطر الأمن السيبراني، أو تطوير قدرات فريق التدقيق الداخلي الحالي في هذا المجال، بحيث يقوم بمراجعات دورية منتظمة (ربع سنوية أو نصف سنوية) لتقييم مدى الالتزام بالسياسات والإجراءات، وفعالية الضوابط المطبقة، ودقة عمليات تحديد وتقييم المخاطر. وينبغي أن ترفع نتائج هذه المراجعات مباشرة إلى الإدارة العليا واللجنة الإدارية لحوكمة الأمن السيبراني، مع خطط عمل واضحة لمعالجة أي ملاحظات أو أوجه قصور مكتشفة. كما يُوصى بالاستعانة بمدققين خارجيين مستقلين بشكل سنوي لإجراء تقييم موضوعي شامل لمنظومة إدارة المخاطر ومقارنتها بأفضل الممارسات والمعايير الدولية، مما يوفر رؤية خارجية نزيهة ويعزز المصداقية.

وعلى مستوى التخطيط الاستراتيجي، توصي الدراسة بتطوير خطة استراتيجية متعددة السنوات (3-5 سنوات) لإدارة مخاطر الأمن السيبراني، تتضمن رؤية واضحة وأهدافاً استراتيجية قابلة للقياس ومبادرات تنفيذية محددة بجداول زمنية وميزانيات ومسؤوليات. يجب أن تكون هذه الخطة متوافقة مع الخطة الاستراتيجية الشاملة للمؤسسة ومرتبطة بأهدافها العليا، وأن تأخذ في الاعتبار التوجهات الوطنية مثل رؤية المملكة 2030 والاستراتيجية الوطنية للأمن السيبراني. ينبغي أن تتضمن الخطة مؤشرات أداء رئيسية (KPIs) واضحة لقياس التقدم المحرز، مثل نسبة الموظفين المدربين، ومعدل تحديث السياسات، ومستوى نضج إدارة المخاطر وفق نماذج معيارية، ومعدلات الحوادث الأمنية واستجابة المؤسسة لها، ودرجة رضا المستفيدين الداخليين والخارجيين عن مستوى الأمن. وينبغي مراجعة هذه الخطة وتحديثها بشكل سنوي لتعكس التغيرات في بيئة التهديدات والأولويات المؤسسية.

وأخيراً على الصعيد الإداري، توصي الدراسة بتعزيز التعاون والتنسيق بين الأقسام المختلفة داخل المؤسسة وكذلك مع المؤسسات الصحية الأخرى والجهات التنظيمية الوطنية. أظهرت نتائج الدراسة أن مشاركة جميع الأقسام في تحديد المخاطر حققت أعلى تقييم في محورها (3.89)، مما يعكس وعياً بأهمية النهج التشاركي، لكن هذا التعاون يحتاج إلى ترسيخه مؤسسياً من خلال آليات واضحة. ينبغي تشكيل فريق عمل متعدد التخصصات لإدارة المخاطر السيبرانية يضم ممثلين دائمين عن الإدارات الحرجة (تقنية المعلومات، الجودة، إدارة المخاطر، الشؤون القانونية، العمليات السريرية، الموارد البشرية)، يجتمع بشكل منتظم لتبادل المعلومات

حول المخاطر والتحديات والحلول، ولضمان أن تعكس سياسات وإجراءات الأمن السيبراني احتياجات جميع الأطراف المعنية. كما يُوصى بالمشاركة الفعالة في المنصات الوطنية والإقليمية لتبادل المعلومات والخبرات في مجال الأمن السيبراني الصحي، مثل تلك التي تنظمها الهيئة الوطنية للأمن السيبراني أو وزارة الصحة، والاستفادة من التنسيق مع المؤسسات الصحية الأخرى لتبادل الدروس المستفادة وأفضل الممارسات، بما يعزز الجاهزية الجماعية للقطاع الصحي ككل.

التوصيات البحثية

إلى جانب التوصيات الإدارية والتنظيمية، تقترح هذه الدراسة عدداً من الاتجاهات البحثية المستقبلية التي يمكن أن تعمق الفهم الأكاديمي والعملية لإدارة مخاطر الأمن السيبراني في القطاع الصحي وتسد الفجوات المعرفية المتبقية.

أولاً: إجراء بحوث طويلة تمتد لعدة سنوات لرصد تطور فعالية ممارسات إدارة مخاطر الأمن السيبراني في المؤسسات الصحية السعودية عبر الزمن. فالدراسة الحالية قدمت صورة مقطعية للوضع في نقطة زمنية واحدة، لكن فهم الديناميكيات الزمنية وأنماط التغيير يتطلب متابعة طويلة الأمد. يمكن لمثل هذه الدراسات أن تكشف عن العوامل المؤسسية التي تسهم في التحسين المستدام، وتقيس تأثير التدخلات والإصلاحات الإدارية على مدى سنوات، وتوفر أدلة أقوى على العلاقات السببية بين المتغيرات. كما أن المقارنة بين المؤسسات التي تحرز تقدماً سريعاً وتلك التي تتعثر يمكن أن تكشف عن عوامل النجاح الحرجة في السياق المحلي.

ثانياً، يُوصى بتوسيع نطاق الدراسات الميدانية جغرافياً ومؤسسياً لتشمل مناطق مختلفة من المملكة وأنواعاً متباينة من المرافق الصحية. اقتصرَت الدراسة الحالية على تجمع نجران الصحي، مما يحد من إمكانية التعميم. دراسات مقارنة تشمل مستشفيات في مدن رئيسية كبرى ومناطق نائية، ومرافق حكومية وخاصة، ومستشفيات كبيرة ومراكز صحية صغيرة، يمكن أن تكشف عن تأثير السياق المحلي والحجم المؤسسي والملكية على ممارسات إدارة المخاطر والتحديات المواجهة. هذا الفهم المقارن ضروري لتطوير سياسات وتوصيات متباينة تناسب السياقات المختلفة بدلاً من نهج واحد يناسب الجميع.

ثالثاً، تدعو الدراسة إلى إجراء بحوث نوعية معمقة تستكشف الجوانب الثقافية والسلوكية والتنظيمية التي تؤثر على إدارة مخاطر الأمن السيبراني في القطاع الصحي السعودي. يمكن للمقابلات المتعمقة مع القيادات الإدارية والعاملين في خطوط المواجهة، ومجموعات التركيز، ودراسات الحالة التفصيلية، أن توفر رؤى غنية لا يمكن للبحث الكمي وحده التقاطها. على سبيل المثال، فهم كيف

تتشكل ثقافة الأمن المؤسسية في السياق السعودي، وما هي العوامل الثقافية المحلية التي تعزز أو تعيق الالتزام بالسياسات الأمنية، وكيف يدرك الموظفون على مستويات مختلفة أدوارهم ومسؤولياتهم في إدارة المخاطر، كلها أسئلة تستحق استكشافاً نوعياً معمقاً يكمل النتائج الكمية للدراسة الحالية.

رابعاً، يُوصى بإجراء دراسات اقتصادية وإدارية تقيّم الجدوى الاقتصادية لاستثمارات الأمن السيبراني في القطاع الصحي والعائد على الاستثمار لبرامج إدارة المخاطر المختلفة. كشفت الدراسة الحالية عن تحدي عدم كفاية الموارد المخصصة، لكن القرارات حول تخصيص الموارد تحتاج إلى أدلة حول التكاليف والعوائد. بحوث تقيس التكلفة الإجمالية لخروقات البيانات والحوادث السيبرانية في المؤسسات الصحية السعودية (تشمل التكاليف المباشرة وغير المباشرة، والخسائر التشغيلية، والأضرار السمعية، والتكاليف القانونية) مقابل تكاليف برامج الوقاية وإدارة المخاطر، يمكن أن توفر مبررات اقتصادية واضحة لصناع القرار لزيادة الاستثمارات في هذا المجال. كما يمكن لدراسات تحليل التكلفة والعائد أن تساعد في تحديد أولويات الاستثمار من خلال مقارنة فعالية وكفاءة التدخلات المختلفة، مثل مقارنة عائد الاستثمار في التدريب المكثف مقابل الاستثمار في تقنيات معينة، أو مقارنة نماذج مختلفة لتوفير الخدمات الأمنية (داخلياً مقابل الاستعانة بمصادر خارجية).

خامساً، توصي الدراسة بتطوير بحوث تركز على قياس وتقييم النضج المؤسسي في إدارة مخاطر الأمن السيبراني باستخدام نماذج نضج معيارية. يمكن تكييف نماذج النضج المعروفة عالمياً مثل نموذج قدرة النضج للأمن السيبراني (C2M2) أو نموذج نضج إدارة المخاطر، بما يتناسب مع السياق الصحي السعودي، ثم استخدامها لتقييم مستوى نضج عينة واسعة من المؤسسات الصحية. هذا النوع من البحوث يمكن أن يوفر معياراً مرجعياً وطنياً (National Benchmark) تستطيع المؤسسات من خلاله قياس موقعها النسبي وتحديد فجواتها، كما يمكن أن يكشف عن العوامل المؤسسية والإدارية المرتبطة بالمستويات الأعلى من النضج، مما يوفر خارطة طريق واضحة للمؤسسات الأقل نضجاً للتحسين.

سادساً، تدعو الدراسة إلى بحوث متعددة التخصصات تجمع بين علوم الإدارة وعلم النفس التنظيمي لفهم العوامل السلوكية والنفسية التي تحدد التزام الأفراد بممارسات إدارة المخاطر السيبرانية. يمكن استخدام نظريات راسخة من علم النفس الاجتماعي مثل نظرية السلوك المخطط (Theory of Planned Behavior) أو نموذج قبول التقنية (Technology Acceptance Model) لدراسة محددات النوايا السلوكية والسلوك الفعلي للموظفين تجاه الامتثال للسياسات الأمنية. فهم هذه الديناميكيات النفسية يمكن أن يساعد في تصميم تدخلات سلوكية أكثر فعالية لتعزيز الالتزام، مثل استخدام

الحوافز المناسبة، أو تصميم رسائل توعوية أكثر إقناعاً، أو معالجة العوائق النفسية التي تمنع الموظفين من اتباع الإجراءات الأمنية.

سابعاً، يُوصى بإجراء دراسات حول الحوكمة والامتثال التنظيمي لمعايير وأطر الأمن السيبراني في القطاع الصحي السعودي. يمكن لهذه البحوث أن تقيّم مدى التزام المؤسسات الصحية بالمتطلبات الوطنية مثل الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، أو بالمعايير الدولية مثل ISO 27001 و HIPAA، وتحديد العوامل التي تسهل أو تعيق الامتثال. كما يمكن لدراسات مقارنة بين الأطر التنظيمية المحلية والدولية أن توفر توصيات لتطوير اللوائح الوطنية بما يحقق التوازن بين الحماية الفعالة والعملية التطبيقية. هذا النوع من البحوث مهم خاصة في ظل التطور المستمر للتشريعات الوطنية المتعلقة بالأمن السيبراني وحماية البيانات.

ثامناً، توصي الدراسة بتطوير بحوث تطبيقية حول أفضل الممارسات الإدارية لإدارة مخاطر الأمن السيبراني في السياق الصحي المحلي. يمكن إجراء دراسات حالة تفصيلية لمؤسسات صحية سعودية رائدة في هذا المجال، لتوثيق ممارساتها الناجحة والعقبات التي تغلبت عليها والدروس المستفادة من تجربتها. هذا النوع من البحوث التطبيقية يوفر نماذج عملية قابلة للتطبيق يمكن للمؤسسات الأخرى الاستفادة منها وتكييفها مع سياقاتها الخاصة. كما يُوصى بإجراء دراسات مقارنة بين نماذج مختلفة لتنظيم وظيفة إدارة المخاطر السيبرانية داخل الهيكل المؤسسي (مركزية مقابل لامركزية، تبعية مباشرة للإدارة العليا مقابل تبعية لإدارة تقنية المعلومات، نماذج هجينة) لتحديد النموذج الأكثر فعالية في السياق الصحي المحلي.

تاسعاً، تدعو الدراسة إلى بحوث حول دور القيادة الإدارية وأنماط القيادة في تعزيز فعالية إدارة مخاطر الأمن السيبراني. رغم أن الدراسة الحالية أكدت أهمية دعم الإدارة العليا، إلا أنها لم تتعمق في كيفية ممارسة هذا الدعم أو الأنماط القيادية الأكثر فعالية في هذا السياق. بحوث تستكشف العلاقة بين أنماط القيادة المختلفة (القيادة التحويلية، التبادلية، الأصلية) وفعالية برامج إدارة المخاطر، أو تدرس كيف يؤثر التزام القيادة ومشاركتها المباشرة على ثقافة الأمن وسلوكيات الموظفين، يمكن أن توفر رؤى قيمة لتطوير القيادات الصحية وإعدادهم لدورهم الحيوي في حماية مؤسساتهم من التهديدات السيبرانية.

عاشرًا، يُوصى بإجراء دراسات حول إدارة التغيير التنظيمي المرتبط بتطبيق أو تطوير ممارسات إدارة المخاطر السيبرانية. أشارت الدراسة الحالية ضمناً إلى وجود تحديات تنظيمية، وقد تشمل هذه التحديات مقاومة التغيير من الموظفين أو القيادات الوسطى. بحوث تطبق نظريات إدارة

التغيير التنظيمي على سياق تحول المؤسسات الصحية نحو ممارسات أمنية أكثر صرامة يمكن أن تكشف عن استراتيجيات فعالة لإدارة المقاومة، وبناء القبول والدعم للتغييرات الأمنية، وضمان التبنى المستدام للممارسات الجديدة.

وأخيراً، توصي الدراسة بجهد بحثي تكاملي على المستوى الوطني لتطوير إطار عمل سعودي شامل لإدارة مخاطر الأمن السيبراني في القطاع الصحي. هذا الجهد البحثي يمكن أن تقوده جامعة أو مركز بحثي بالتعاون مع الجهات التنظيمية مثل وزارة الصحة والهيئة الوطنية للأمن السيبراني، ويهدف إلى تطوير إطار موحد يأخذ في الاعتبار خصوصيات السياق المحلي (الثقافة التنظيمية، البنية التشريعية، التحديات الفريدة) بينما يتوافق مع المعايير والممارسات العالمية. يجب أن يكون هذا الإطار مدعوماً بأدلة علمية من دراسات ميدانية محلية واسعة، وأن يتضمن مكونات إدارية وتنظيمية وبشرية إلى جانب المكونات التقنية، بحيث يكون قابلاً للتطبيق في مختلف أنواع المؤسسات الصحية ويوفر معياراً مرجعياً وطنياً للتميز في هذا المجال.

وفي الختام، تمثل التوصيات الإدارية والبحثية المطروحة في هذه الدراسة خارطة طريق متكاملة لتطوير وتعزيز منظومة إدارة مخاطر الأمن السيبراني في القطاع الصحي السعودي من منظور إداري وتنظيمي. التوصيات الإدارية تركز على الجوانب القابلة للتنفيذ الفوري من قبل القيادات والمديرين في المؤسسات الصحية، وتعالج التحديات المحددة التي كشفت عنها الدراسة الحالية مثل تخصيص الموارد، والتدريب، وتحديث السياسات، والمساءلة، وبناء الثقافة المؤسسية. هذه التوصيات ليست تقنية بحتة، بل تركز على الأبعاد الإدارية والتنظيمية والبشرية التي أثبتت الدراسة أنها محددات جوهرية لنجاح أو فشل برامج إدارة المخاطر السيبرانية.

أما التوصيات البحثية فتفتح آفاقاً واسعة لتعميق المعرفة الأكاديمية والعملية في هذا المجال الحيوي والمتطور، من خلال معالجة الفجوات المعرفية المتبقية واستكشاف أبعاد جديدة لم تتناولها الدراسة الحالية. هذه التوصيات البحثية موجهة للباحثين الأكاديميين والمراكز البحثية والجامعات، وتشمل مجالات متنوعة من الدراسات الطولية والمقارنة والنوعية والاقتصادية والتطبيقية، بما يثري قاعدة الأدلة العلمية ويدعم صناعة القرار المبني على البحث.

إن تبني هذه التوصيات على المستويين العملي والبحثي من قبل صناع القرار والممارسين والباحثين سيسهم بشكل فعال في تحقيق الهدف الاستراتيجي المتمثل في بناء قطاع صحي آمن رقمياً، قادر على حماية بيانات المرضى الحساسة، وضمان استمرارية الخدمات الحيوية في مواجهة التهديدات السيبرانية المتصاعدة والمتطورة. هذا الهدف ليس مجرد متطلب تقني أو أمني، بل هو ضرورة أخلاقية ومهنية تنبع من صميم رسالة القطاع الصحي في رعاية المرضى وحمايتهم. كما أنه يتماشى بشكل كامل مع التوجهات الاستراتيجية

الوطنية التي تجسدها رؤية المملكة 2030 والاستراتيجية الوطنية للأمن السيبراني، والتي تضع الأمن الرقمي كأولوية وطنية وعامل تمكين أساسي للتحول الرقمي الشامل في جميع القطاعات.

ختاماً، فإن النجاح في تطبيق هذه التوصيات يتطلب التزاماً مؤسسياً حقيقياً من القيادات العليا، وتخصيصاً كافياً للموارد، وتعاوناً فعالاً بين جميع الأطراف المعنية داخل المؤسسات الصحية وعبرها، وجهداً بحثياً مستمراً لتطوير المعرفة وتقييم الفعالية. إدارة مخاطر الأمن السيبراني ليست مشروعاً لمرة واحدة أو مسؤولية قسم واحد، بل هي رحلة مستمرة من التحسين والتطوير تتطلب يقظة دائمة واستعداداً للتكيف مع المتغيرات. والمؤسسات الصحية التي تنجح في دمج إدارة المخاطر السيبرانية في صميم ثقافتها وعملياتها واستراتيجياتها ستكون الأكثر قدرة على تحقيق رسالتها في خدمة المرضى والمجتمع بأمان وثقة في العصر الرقمي.

المراجع

المراجع العربية

- الرحاحله, أ. م. ا. (2025). دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني. *Humanitarian and Natural Sciences Journal*, 6(10).
<https://doi.org/10.53796/hnsj610/23>
- الشهري, ر. & سلمان, د. (2024). دور إدارة المخاطر في الرعاية الافتراضية على جودة المخرجات الصحية: دراسة تطبيقية على مستشفى صحة الافتراضي بالمملكة العربية السعودية. *المجلة العربية للإدارة*, 0(0), 1–16. <https://doi.org/10.21608/aja.2024.323466.1724>
- المرداس, ن. (2023). الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية). *International Journal of Research and Studies Publishing*, 5(49), 204–225. <https://doi.org/10.52133/ijrsp.v5.49.8>
- عفيفي, آ. أ. ع. م. (2024). تأثير تطبيق إدارة المخاطر على مشاريع الرعاية الصحية: دراسة تطبيقية على مستشفيات في جدة. *المجلة الدولية للبحوث العلمية*, 8(3), 860–892. <https://doi.org/10.59992/IJSR.2024.V3N8P24>
- وزارة الصحة السعودية. (2024). *الكتاب الإحصائي السنوي*.

المراجع الأجنبية

- Alder, S. (2025). *Healthcare Data Breach Statistics*.
<https://www.hipaajournal.com/healthcare-data-breach-statistics/>
- Aldosari, B. (2025). Cybersecurity in Healthcare: New Threat to Patient Safety. *Cureus*, 17(5), e83614. <https://doi.org/10.7759/CUREUS.83614>
- Alharthi, G. (2021). *Saudi Arabia's Vision 2030 aims to empower the non-profit sector*.
<https://www.atlanticcouncil.org/blogs/menasource/saudi-arabias-vision-2030-aims-to-empower-the-non-profit-sector-here-are-three-areas-to-focus-on/>
- Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & Alduaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. *Applied Clinical Informatics*, 12(4), 924. <https://doi.org/10.1055/S-0041-1735527>
- Archer, L. (2023). Research methodology: A step-by-step guide for beginners (5th. ed.). *Journal of Latinos and Education*, 22(1), 425–426.
<https://doi.org/10.1080/15348431.2019.1661251>
- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020).

Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1).
<https://doi.org/10.1186/S12911-020-01161-7>

- Božić, V. (2024). Cybersecurity Governance in Healthcare: A Comprehensive Overview. *General Hospital Koprivnica*. <https://www.researchgate.net/publication/381193427>
- Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, 24(1), 133. <https://doi.org/10.1186/S12911-024-02551-X>
- Clarke, M., & Martin, K. (2023). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, 37(1), 17. <https://doi.org/10.1177/08404704231195804>
- Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *Digital Health*, 11, 20552076251343960. <https://doi.org/10.1177/20552076251343959>
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
- Creswell, J. W. ., & Creswell, J. David. (2023). *Research design : qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.
- Dawood Ahmed Rihan, S. (2025). Awareness and Challenges of adopting Cybersecurity at health colleges at Najran University. *Egyptian Journal of Health Care*, 16(1), 472–481. <https://doi.org/10.21608/ejhc.2025.414466>
- Definitive Healthcare. (2024). *Most Common Types of Healthcare Data Breaches | Data Security*. <https://www.definitivehc.com/resources/healthcare-insights/most-common-healthcare-data-breaches>
- Field, A. P. . (2013). *Discovering statistics using IBM SPSS statistics*. SAGE.
- Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*, 2(1), 98. <https://doi.org/10.1038/S41746-019-0161-6>
- Grande, D., Luna Marti, X., Feuerstein-Simon, R., Merchant, R. M., Asch, D. A., Lewson, A., & Cannuscio, C. C. (2020). Health Policy and Privacy Challenges Associated With Digital Technology. *JAMA Network Open*, 3(7), e208285. <https://doi.org/10.1001/jamanetworkopen.2020.8285>
- Hakami, N., Alshareef, H., & Helal, M. (2024). A security framework to protect ePHI in Saudi Arabia's healthcare infrastructure. *International Journal of Advanced and Applied Sciences*, 11(4), 167–181. <https://doi.org/10.21833/IJAAS.2024.04.019>
- HIMSS. (2024). *HIMSS Cybersecurity Survey*.
- IBM. (2025). *Cost of a data breach 2025 | IBM*. <https://www.ibm.com/reports/data-breach>
- Kanaan, A. G., AL-Hawamleh, A. M., Jaradat, Z. A., Alorfi, A. S., Alqudah, M. K., Alqudah, M. K., & Abualigah, L. (2024). *Towards Business Continuity Management in the Saudi*

Healthcare Sector Through Security and Operational Risk Management.

<https://doi.org/10.2139/SSRN.5071177>

- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. <https://doi.org/10.3233/THC-161263>
- Kumar, Ranjit. (2019). *Research methodology : a step-by-step guide for beginners*. SAGE.
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9. <https://doi.org/10.3233/THC-151102>
- Mani, Z. A., & Goniewicz, K. (2024). Transforming Healthcare in Saudi Arabia: A Comprehensive Evaluation of Vision 2030's Impact. *Sustainability*, 16(8), 3277. <https://doi.org/10.3390/su16083277>
- Mirzaei, A., Mohammadi, A., Bouraghi, H., Mohammadpour, A., Mohamadyari, E., Lotfi, S., & Shanbehzadeh, M. (2020). Evaluation of Hospital Information System of hospitals Affiliated. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 19, Issue 1). <https://www.researchgate.net/publication/339017457>
- Molosiwa, T., & Molosiwa, T. (2025). Risk Management Systems in Healthcare: Insights and Challenges for Adoption—A Systematic Analysis. *Journal of Service Science and Management*, 18(2), 39–53. <https://doi.org/10.4236/JSSM.2025.182004>
- NHCAA. (2022). *The Challenge of Health Care Fraud – NHCAA*. <https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/>
- Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, 74, 102719. <https://doi.org/10.1016/j.ijinfomgt.2023.102719>
- Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study. *JMIR Formative Research*, 7, e41738. <https://doi.org/10.2196/41738>
- Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*, 8, 20552076221081716. <https://doi.org/10.1177/20552076221081716>
- Saudi Healthcare Consulting. (2024). *Protecting Patient Data: Saudi Cybersecurity Measures*. <https://saudihealthcareconsulting.com/insights/articles/protecting-patient-data-saudi-cybersecurity-measures>
- Saunders, M. N. K. ., Lewis, Philip., & Thornhill, Adrian. (2023). *Research methods for business students*. Pearson.
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8(2), 133. <https://doi.org/10.3390/HEALTHCARE8020133>
- Sekaran, Uma., & Bougie, Roger. (2016). *Research methods for business : a skill-building approach*. John Wiley & Sons.

- Shadadi, E., Ibrahim, R., & Ghadafi, E. (2025). Cybersecurity Threats in Saudi Healthcare: Exploring Email Communication Practices to Enhance Cybersecurity Among Healthcare Employees in Saudi Arabia. *Computers*, 14(8), 324.
<https://doi.org/10.3390/computers14080324>
- Whitman, M. E. ., & Mattford, H. J. . (2019). *Management of information security*. Cengage Learning.
- Williams, P. A., Lovelock, B., Cabarrus, T., & Harvey, M. (2019a). Improving Digital Hospital Transformation: Development of an Outcomes-Based Infrastructure Maturity Assessment Framework. *JMIR Medical Informatics*, 7(1), e12465.
<https://doi.org/10.2196/12465>
- Williams, P. A., Lovelock, B., Cabarrus, T., & Harvey, M. (2019b). Improving Digital Hospital Transformation: Development of an Outcomes-Based Infrastructure Maturity Assessment Framework. *JMIR Medical Informatics*, 7(1), e12465.
<https://doi.org/10.2196/12465>

الملاحق

ملحق (1): الاستبانة النهائية للدراسة

استبانة: تقييم ممارسات إدارة مخاطر الأمن السيبراني وأثرها على حماية بيانات المرضى واستمرارية الخدمات الصحية - تجمع نجران الصحي

أولاً: مقدمة الاستبانة

السادة المشاركون الكرام،

تهدف هذه الاستبانة إلى جمع بيانات بحثية حول مدى تطبيق ممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي، ودراسة أثرها على كلّ من حماية بيانات المرضى و استمرارية الخدمات الصحية، بالإضافة إلى التعرف على التحديات التنظيمية والبشرية المرتبطة بتطبيق هذه الممارسات.

تُستخدم البيانات لأغراض بحثية فقط، وتُعامل بسرية تامة، ولن يُطلب منكم أي معلومات شخصية يمكن أن تكشف هويتكم.

مشاركاتكم ستسهم في تطوير مستوى الأمن السيبراني وتحسين جودة الخدمات الصحية.

شاكرين لكم تعاونكم.

ثانياً: الموافقة المستنيرة

- ✓ أقرّ بأن مشاركتي تطوعية تماماً.
- ✓ أفهم أن البيانات ستُستخدم لأغراض البحث العلمي فقط.
- ✓ أفهم أنه يمكنني الانسحاب في أي وقت دون أي تبعات.
- ✓ أوافق على المشاركة في هذا البحث.

هل توافق على المشاركة؟

- () نعم
- () لا → تنتهي الاستبانة هنا

ثالثاً: التعليمات

- يرجى قراءة كل عبارة بدقة واختيار مستوى موافقتك وفق مقياس ليكرت الخماسي التالي:

1 = لا أوافق بشدة

2 = لا أوافق

3 = محايد

4 = أوافق

5 = أوافق بشدة

القسم الأول: البيانات الديموغرافية والمهنية

1. الجنس:

• () ذكر

• () أنثى

2. العمر:

• () أقل من 24 سنة

• () 24-29 سنة

• () 30-39 سنة

• () 40-49 سنة

• () 50-55 سنة

• () 55 فأكثر

3. المؤهل العلمي:

• () شهادة ثانوية / دبلوم

• () بكالوريوس

• () ماجستير

• () دكتوراه

4. المسمى الوظيفي:

• () تقنية معلومات

• () إداري

• () طبي

5. سنوات الخبرة:

• () أقل من 5 سنوات

• () 5-10 سنوات

• () 11-15 سنة

• () أكثر من 15 سنة

القسم الثاني: ممارسات إدارة مخاطر الأمن السيبراني

أولاً: البعد 1 - تحديد المخاطر (Risk Identification - RI)

رقم	العبارة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
1	توجد آليات واضحة لتحديد المخاطر السيبرانية	RI1	☐	☐	☐	☐	☐
2	يتم تحديث قائمة المخاطر بشكل دوري	RI2	☐	☐	☐	☐	☐
3	تشمل عملية تحديد المخاطر جميع الأنظمة والبيانات	RI3	☐	☐	☐	☐	☐
4	تشارك جميع الأقسام المعنية في تحديد المخاطر	RI4	☐	☐	☐	☐	☐

ثانياً: البعد 2 - تقييم المخاطر (Risk Assessment - RA)

رقم	العبارة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
5	يتم تقييم احتمالية حدوث كل خطر سيبراني.	RA1	☐	☐	☐	☐	☐
6	يتم تقييم أثر الهجمات السيبرانية المحتمل.	RA2	☐	☐	☐	☐	☐
7	يوجد تصنيف للمخاطر وفق خطورتها.	RA3	☐	☐	☐	☐	☐
8	تعتمد المنشأة تقارير تقييم مبنية على معايير دولية.	RA4	☐	☐	☐	☐	☐

ثالثاً: البعد 3 - معالجة المخاطر (Risk Treatment - RT)

رقم	العبارة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
9	توجد خطط واضحة لمعالجة المخاطر المحددة	RT1	☐	☐	☐	☐	☐

10	يتم تخصيص الموارد الكافية لتنفيذ خطط المعالجة	RT2	○	○	○	○	○
11	يتم متابعة تنفيذ إجراءات المعالجة بانتظام	RT3	○	○	○	○	○
12	توجد بدائل متعددة لمعالجة كل خطر	RT4	○	○	○	○	○

رابعاً: البعد 4 – متابعة ومراجعة المخاطر (Monitoring & Review – MR)

رقم	العبرة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
13	توجد آليات مراقبة مستمرة للتهديدات السيبرانية ويتم اختبار الأنظمة بشكل دوري.	MR1	○	○	○	○	○
14	يتم إجراء مراجعات دورية لفعالية الضوابط الأمنية	MR2	○	○	○	○	○
15	توجد تقارير منتظمة عن حالة الأمن السيبراني	MR3	○	○	○	○	○
16	يتم التعامل الفوري مع أي انحرافات أمنية مكتشفة	MR4	○	○	○	○	○

القسم الثالث: حماية بيانات المرضى (Patient Data Protection – PDP)

رقم	العبرة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
17	يتم تشفير بيانات المرضى أثناء التخزين والنقل	PDP1	○	○	○	○	○
18	توجد ضوابط صارمة للتحكم في الوصول لبيانات المرضى	PDP2	○	○	○	○	○
19	يتم مراجعة صلاحيات الوصول بشكل دوري	PDP3	○	○	○	○	○
20	توجد آليات للكشف عن محاولات الوصول غير المصرح بها	PDP4	○	○	○	○	○
21	يتم النسخ الاحتياطي للبيانات بشكل منتظم	PDP5	○	○	○	○	○
22	توجد خطط لاستعادة البيانات في حالة فقدانها	PDP6	○	○	○	○	○
23	يلتزم الموظفون بسياسات حماية خصوصية المرضى	PDP7	○	○	○	○	○

القسم الرابع: استمرارية الخدمات الصحية (Service Continuity – SC)

رقم	العبرة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
24	لدى المنشأة خطة استمرارية أعمال محدثة.	SC1	○	○	○	○	○
25	يتم اختبار خطة الاستمرارية بشكل دوري.	SC2	○	○	○	○	○
26	الأنظمة الحيوية لها بدائل تشغيلية.	SC3	○	○	○	○	○
27	يتم الحد من فترات توقف الخدمة.	SC4	○	○	○	○	○

○	○	○	○	○	SC5	توجد إجراءات لضمان استمرار العمل أثناء الهجمات.	28
○	○	○	○	○	SC6	تتوفر بنية تحتية مرنة لاستعادة الخدمة.	29
○	○	○	○	○	SC7	تتكامل خطة الاستمرارية مع إدارة المخاطر السيبرانية.	30

القسم الخامس: التحديات التنظيمية والبشرية (Organizational & Human Challenges – CH)

رقم	العبرة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
31	يوجد نقص في كوادرات الأمن السيبراني.	CH1	○	○	○	○	○
32	ميزانية الأمن السيبراني غير كافية.	CH2	○	○	○	○	○
33	برامج التدريب غير كافية.	CH3	○	○	○	○	○
34	توجد مقاومة للتغيير التقني.	CH4	○	○	○	○	○
35	ضعف الوعي الأمني يرفع مستوى المخاطر.	CH5	○	○	○	○	○
36	توجد صعوبة في تطبيق اللوائح الأمنية.	CH6	○	○	○	○	○
37	التواصل بين الإدارات بشأن الأمن السيبراني ضعيف.	CH7	○	○	○	○	○

القسم السادس: الرضا العام عن منظومة الأمن السيبراني SAT

رقم	العبرة	الكود	لا أوافق بشدة	لا أوافق	حيادي	أوافق	أوافق بشدة
38	أشعر بالثقة في قدرة المؤسسة على حماية البيانات	SAT1	○	○	○	○	○
39	الممارسات الحالية كافية لمواجهة التهديدات السيبرانية	SAT2	○	○	○	○	○
40	أرى تحسناً مستمراً في مستوى الأمن السيبراني	SAT3	○	○	○	○	○

المستخلص

استهدفت هذه الدراسة تقييم فاعلية منظومة إدارة مخاطر الأمن السيبراني كعملية إدارية استراتيجية في القطاع الصحي، من خلال فحص العلاقة بين أبعادها الأربعة (تحديد المخاطر، تقييم المخاطر، معالجة المخاطر، والمراقبة على المخاطر) وتحقيق هدفين تنظيميين حرجين: حماية بيانات المرضى واستمرارية الخدمات الصحية. أجريت الدراسة في تجمع نجران الصحي باستخدام المنهج الوصفي التحليلي على عينة طبقية من 233 مشاركاً عبر مستويات تنظيمية متعددة، وحقت الأداة معامل ثبات ($\alpha=0.947$).

كشفت النتائج عن مستوى نضج إداري متقدم في ممارسات إدارة المخاطر بالتجمع، حيث حققت جميع الأبعاد مستويات أداء مرتفعة (متوسطات 3.60-3.87 من 5)، مع تميز واضح في محور حماية بيانات المرضى (3.87). أثبت بُعد معالجة المخاطر التأثير الأقوى على المخرجات التنظيمية ($\text{Beta}=0.294$)، مما يؤكد نجاح التجمع في التنفيذ العملي لاستراتيجيات إدارة المخاطر. كما أظهر تحليل الانحدار المتعدد أن الأبعاد الأربعة تعمل بتكامل منهجي، وتفسر مجتمعة 61.1% من التباين في فعالية حماية البيانات و51.0% من التباين في استمرارية الخدمات.

أثبتت الدراسة وجود علاقات ارتباطية قوية ودالة إحصائياً بين فعالية ممارسات إدارة المخاطر وكل من حماية بيانات المرضى ($r=0.726, p<0.001$) واستمرارية الخدمات ($r=0.714, p<0.001$)، مما يؤكد أن الاستثمار الإداري في منظومة إدارة المخاطر ينعكس مباشرة على تحقيق الأهداف التنظيمية الاستراتيجية. كما سجل التجمع مستوى رضا مرتفع من العاملين (3.79)، مما يعكس ثقة مؤسسية إيجابية في الإجراءات المتبعة.

حددت الدراسة ثلاثة مجالات استراتيجية للتحسين المستمر يمكن أن تعزز من فعالية المنظومة: تعظيم الاستفادة من الموارد المالية ($\text{Beta}=0.276$)، وتطوير آليات التنسيق بين الوحدات التنظيمية ($\text{Beta}=0.271$)، والاستثمار المستمر في تنمية رأس المال البشري ($\text{Beta}=0.257$). أظهر التحليل أن التدريب والتطوير المهني يحقق تأثيراً ملموساً (فرق 0.34 نقطة)، مما يبرز أهمية الاستثمار في الكفاءات كرافعة للتميز المؤسسي.

بناءً على الإنجازات المتحققة، توصي الدراسة بمسارات تطويرية استراتيجية تشمل: تطوير إطار حوكمة متقدم، وبلورة استراتيجية خمسية طموحة مرتبطة بمؤشرات أداء متقدمة، وتعزيز الاستثمار في الأمن السيبراني (10-12% من ميزانية تقنية المعلومات)، وتوسيع برامج التطوير المهني، وتبني منهجية التحسين المستمر. تقدم هذه الدراسة نموذجاً تطبيقياً متقدماً يدعم رؤية المملكة 2030 في بناء قطاع صحي رقمي آمن ومستدام، وتوفر أدلة تجريبية قوية لصناع القرار في رحلة الارتقاء بفعالية إدارة مخاطر الأمن السيبراني نحو مستويات الريادة العالمية.

الكلمات المفتاحية: إدارة المخاطر، إدارة مخاطر الأمن السيبراني، حماية بيانات المرضى، استمرارية الخدمات الصحية، تجمع نجران الصحي، القطاع الصحي السعودي.

Abstract

This study evaluated the effectiveness of cybersecurity risk management as a strategic administrative process in healthcare, examining the relationship between its four dimensions (risk identification, assessment, treatment, and monitoring) and achieving two critical organizational objectives: patient data protection and health services continuity. Conducted at Najran Health Cluster using a descriptive-analytical approach with a stratified sample of 233 participants across multiple organizational levels, the instrument achieved reliability ($\alpha=0.947$).

Results revealed advanced administrative maturity in the cluster's risk management practices, with all dimensions achieving high performance levels (means 3.60-3.87/5), demonstrating particular excellence in patient data protection (3.87). Risk treatment showed the strongest impact on organizational outcomes (Beta=0.294), confirming successful operational execution of risk management strategies. Multiple regression analysis demonstrated systematic integration of the four dimensions, collectively explaining 61.1% of variance in data protection effectiveness and 51.0% in service continuity.

The study confirmed strong statistically significant correlations between risk management practices effectiveness and both patient data protection ($r=0.726$, $p<0.001$) and service continuity ($r=0.714$, $p<0.001$), validating that administrative investment in risk management directly achieves strategic organizational objectives. The cluster recorded high staff satisfaction (3.79), reflecting positive institutional confidence.

Three strategic improvement areas were identified to enhance system effectiveness: maximizing financial resource utilization (Beta=0.276), developing inter-unit coordination mechanisms (Beta=0.271), and sustained human capital investment (Beta=0.257). Analysis showed training and professional development achieve tangible impact (0.34-point difference), highlighting competency investment as an institutional excellence lever.

Based on achievements, the study recommends strategic developmental pathways including: developing advanced governance framework, formulating ambitious five-year strategy with advanced KPIs, enhancing cybersecurity investment (10-12% of IT budget), expanding professional development programs, and adopting continuous improvement methodology. This research presents an advanced applied model supporting Saudi Vision 2030 in building a secure and sustainable digital healthcare sector, providing strong empirical evidence for decision-makers in elevating cybersecurity risk management effectiveness toward global leadership levels.

Keywords: Risk Management, Cybersecurity Risk Management, Patient Data Protection, Continuity of Health Services, Najran Health Cluster, Saudi Health Sector.