

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

إعداد الطالبه :

شذى ناصر اللافى

إشراف

د. الفصيل عبد الحميد

د. فايز جراد

العام الدراسي

2025

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 أُلغيت 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 كُشف 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 (Saudi Healthcare Consulting, 2024). من 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 (HIMSS, 2024). 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 (إحدى 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. في هذا السياق، برزت **مشكلة البحث** المتمثلة في الحاجة إلى تقييم مدى فعالية ممارسات إدارة مخاطر الأمن السيبراني المطبقة في المؤسسات الصحية لحماية بيانات المرضى وضمان استمرار الخدمة بشكل موثوق. على مستوى تجمع نجران الصحي خصوصاً، حيث تثار مجموعة من التساؤلات الهامة التي تعكس جوانب المشكلة:

- **ما هي ممارسات إدارة مخاطر الأمن السيبراني الحالية في تجمع نجران الصحي؟** تتنبثق 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. على سبيل المثال، أدت هجومات **الفدية الإلكترونية** مثل هجوم *WannaCry* عام 2017 إلى تعطيل خدمات صحية وتأجيل إجراءات طبية في العديد من الدول (Riggi, 2023)، 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 والتقصي العلمي في بيئة تجمع نجران الصحي، مما يسهم في تعزيز أمن المعلومات الصحية والموثوقية التشغيلية.

أهمية الدراسة

تتبع 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 – سواء 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 (كالتهجير 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 تحدّ 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 تتبثق عنه عدة أسئلة فرعية تغطي مختلف جوانب الموضوع محل البحث. السؤال الرئيسي للدراسة هو:

إلى أي مدى تساهم ممارسات إدارة مخاطر الأمن السيبراني المطبقة في تجمع نجران الصحي في حماية بيانات المرضى وضمان استمرارية الخدمات الصحية؟
ويتفرع 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 يُعتد به إحصائياً.

الدراسات السابقة:

تشكل 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

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 تشدد 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.

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 لتزايد وتيرة الهجمات الإلكترونية التي تستهدف البيانات الطبية القيمة. 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 مطرد 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 أكدت 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.

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 يعرض 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. وتتبع الدراسات الحديثة إلى ضرورة دمج إدارة مخاطر الأمن السيبراني ضمن إطار إدارة استمرارية الأعمال في القطاع الصحي (Kanaan et al., 2024)، 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).

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 ممنهجاً 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 وقر 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 والطب 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 ويُحسّن 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 يحذّر 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 مباشرة بالأمن السيبراني الصحي، كما أن استخدام المنهج الإحصائي المتقدم منح المخرجات

مصادقية 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 بالمطلوبات التنظيمية الأساسية. لكن في المقابل، تبين أن عمليات تحديد المخاطر وتقييمها تفتقر 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 يضيف 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 أن 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 المصاحب بالتغذية الراجعة على رفع يقظة العاملين وتقليل الأخطاء البشرية المرتبطة بالتصيد.

وفي سياقٍ عربي، قدّمت الدراسة (Alhuwail et al., 2021) مسحاً على 453 من العاملين في مرافق صحية كويتية، كاشفةً أن الممارسة الآمنة للمعلومات ترتبط بعوامل ديموغرافية؛ حيث تفوّق 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 و 4.06 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، لكنها 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 مكامن 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 معمّقة من واقع خبراء الممارسة، مما يضفي 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 السببراني 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 يمهد تحديدها لبلورة مساهمة البحث الحالي. يوضح الجدول أدناه تلخيصاً موضوعياً مقارناً لأبرز النتائج من الدراسات السابقة، مجمعة حسب محاور التركيز الرئيسية:

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.

• 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.	(Rizzoni et al., 2022) Alhuwail et al.,) (2021 Dawood Ahmed) (Rihan, 2025	العوامل البشرية والتوعية
• تكامل إدارة المخاطر مع استمرارية الأعمال أثبت فعاليته: 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. بيّنت 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.	(Kanaan et al., 2024) (Burke et al., 2024)	استمرارية الخدمة والمرونة التشغيلية

• 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.		
---	--	--

من الجدول والتحليل أعلاه، يمكن تلمس 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 بوزيتش) أن الالتزام بالمعايير مثل HIPAA و GDPR يساهم في حماية البيانات وبناء الثقة مع المرضى، لكنه وحده غير كافٍ ما لم يتم تبنيه ضمن استراتيجية أمنية أوسع نطاقاً تشمل إدارة نشطة 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 إلى 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 تغطِ 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 نتائجه الفجوة بين التوصيات النظرية والتطبيق العملي في ميدان أمن المعلومات الصحي.

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.

المنهجية وطرق البحث

اعتمدت هذه الدراسة منهجية علمية وصفية تحليلية تهدف إلى دراسة الظاهرة كما توجد في الواقع وتفسيرها اعتماداً على البيانات الفعلية من الميدان. يتيح المنهج الوصفي التحليلي للباحث فهم أسباب الظاهرة وتبعاتها من خلال وصف دقيق لكافة خصائصها وعلاقاتها، بما يساعد في اقتراح حلول عملية مبنية على الأدلة. وقد تم اختيار هذا المنهج لمرونته وشموليته في دراسة مشكلات الإدارة والرعاية الصحية، حيث يُمكن الباحث من الجمع بين التحليل الكمي والكيفي لفهم أبعاد مشكلة الأمن السيبراني في البيئة الصحية المحلية. اتّبع تصميم البحث الخطوات العلمية الموصى بها في بحوث الإدارة والمخاطر، بدءاً من تحديد مشكلة الدراسة وصياغة أسئلتها بوضوح، مروراً بوضع فرضيات الدراسة، وبناء إطار نظري يستند إلى أحدث المراجع العلمية ذات الصلة، ووصولاً إلى تصميم إجراءات جمع البيانات وتحليلها. فيما يلي توضيح لعناصر منهجية البحث وطرائقه:

- **فرضيات الدراسة وتصميمها:** انطلقت الدراسة من فرضية رئيسية مؤداها أن ممارسات إدارة مخاطر الأمن السيبراني المطبقة في تجمع نجران الصحي ذات فاعلية إيجابية في حماية بيانات المرضى وضمان استمرارية الخدمات. من هذه الفرضية العامة، تفرعت فرضيات فرعية مرتبطة بأسئلة الدراسة - على سبيل المثال، تم افتراض وجود مستوى عالٍ من تطبيق الضوابط الأمنية التقنية والإدارية في التجمع الصحي، كما تم افتراض وجود تأثير إيجابي لهذه الضوابط على تقليل حوادث اختراق البيانات وتقليل فترات تعطّل الخدمة عند حدوث الحوادث السيبرانية. صُمم البحث بطريقة دراسة ميدانية مسحية في بيئة تجمع نجران الصحي، مما يعني جمع البيانات مباشرة من الواقع العملي بالمؤسسة وتحليلها إحصائياً بهدف استنباط استنتاجات قابلة للتعميم على بيئات مشابهة. تمت هيكلة البحث بحيث يسمح باختبار الفرضيات من خلال الأدلة الميدانية: إذ تم تحديد متغيرات مستقلة (مثل مستوى تطبيق سياسات الأمن، وكفاءة البنية التحتية التقنية، ودرجة وعي الموظفين بالأمن السيبراني) ومتغيرات تابعة (مثل معدل حوادث الاختراق، ومدة التوقف في الخدمات الصحية أثناء الهجمات، ومستوى الامتثال للمعايير الأمنية). تم تصميم نموذج البحث لقياس العلاقات بين هذه المتغيرات باستخدام أدوات إحصائية مناسبة لفحص الفرضيات، مثل اختبار معاملات الارتباط واختبارات الفروق الإحصائية إذا اقتضت الحاجة.

- **المجتمع الإحصائي وعينة الدراسة:** يتألف المجتمع الإحصائي المستهدف من جميع الأفراد والجهات المعنية بتطبيق أمن المعلومات والرعاية الصحية في تجمع نجران الصحي. ويشمل ذلك الإداريين في مجال تقنية المعلومات وإدارة المخاطر، وموظفي الأمن السيبراني، وربما بعض الكوادر الطبية والإدارية الذين لديهم دراية أو دور في سياسات حماية بيانات المرضى. نظراً لصعوبة دراسة المجتمع بأكمله عملياً، اعتمدت الدراسة على عينة ممثلة لهذا المجتمع. سيتم تحديد حجم العينة باستخدام الأساليب الإحصائية الملائمة لضمان تمثيل كافي وموثوق (حيث سيتم استخدام معادلات

تقدير الحجم للعينة على أساس حجم المجتمع ومستوى الثقة المطلوب وهوامش الخطأ المقبولة). كما سيتم مراعاة تنوع المشاركين عند اختيار العينة بحيث تشمل مختلف الأقسام والمستويات الوظيفية ذات العلاقة بموضوع الدراسة، وذلك لضمان شمولية النتائج. تم استخدام أسلوب المعاينة الطبقيّة العشوائية، حيث قُسم المجتمع إلى فئات (مثل: قسم تقنية المعلومات، إدارة المستشفيات، الأقسام الإكلينيكية الرئيسية)، ثم سيتم عينة عشوائية من كل فئة بنسبة تتناسب مع حجمها في المجتمع الكلي. يهدف هذا الأسلوب إلى زيادة تمثيل العينة لكافة جوانب المجتمع وتحقيق قدر أكبر من الدقة في النتائج.

• **أدوات جمع البيانات وطرقها:** تستخدم الدراسة الاستبانة (Questionnaire) كأداة رئيسية لجمع البيانات من أفراد العينة، وهي أداة شائعة وفعّالة في البحوث الوصفية الميدانية. وسيتم تصميم الاستبانة خصيصاً لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها، بحيث تشمل مجموعة من الأسئلة المغلقة التي تغطي المحاور التالية: مستوى تطبيق سياسات وإجراءات الأمن السيبراني، مدى توفر الضوابط التقنية (كأنظمة الحماية والتشفير والنسخ الاحتياطي)، مستوى تدريب العاملين ووعيهم بسياسات الأمن، عدد وتكرار حوادث الاختراق أو تعطل الأنظمة خلال الفترة السابقة، وفعالية خطط الاستجابة والطوارئ المطبقة. كما سيتم إعداد أسئلة الاستبانة بصيغة ليكرت الخماسية لقياس درجة الموافقة أو التقييم الكمي من قبل المشاركين على عبارات تتعلق بكل محور (مثل: مدى الاتفاق مع عبارة "تطبق المنشأة نظام إدارة مخاطر سيبرانية شامل بفعالية"). ولضمان صدق الأداة (Validity) سيتم عرض نسخة أولية من الاستبانة على مجموعة من المحكمين الخبراء في مجالات إدارة المخاطر والأمن السيبراني والرعاية الصحية، بهدف مراجعة الأسئلة من حيث الوضوح والشمولية وملاءمتها لموضوع الدراسة. كما سيتم إجراء اختبار استطلاعي (Pilot Test) بتطبيق الاستبانة بشكل محدود على عينة صغيرة ممثلة للتأكد من وضوح الأسئلة وسهولة الإجابة عنها، ولحساب ثبات الأداة (Reliability) باستخدام معامل كرنباخ ألفا لقياس الاتساق الداخلي لمحاور الاستبانة.

• **إجراءات جمع البيانات:** بعد تصميم الاستبانة والتحقق من صلاحيتها، سيتم توزيعها على أفراد العينة المختارة خلال الفترة الزمنية المحددة للدراسة، وسيتم اتباع طرق متعددة في التوزيع لضمان الحصول على قدر كافٍ من الردود، بما في ذلك التوزيع الورقي المباشر في مقرات العمل والمستشفيات التابعة لتجمع نجران الصحي، وكذلك توفير نسخة إلكترونية عبر البريد الإلكتروني أو منصات الاستبيانات الإلكترونية الآمنة لتسهيل مشاركة المستجيبين. وسيرافق عملية التوزيع خطاب يوضح هدف الدراسة ويؤكد على سرية إجابات المشاركين واستخدامها للأغراض البحثية فقط، وذلك لتشجيعهم على الرد بصراحة ودقة. كما تم التنسيق مسبقاً مع إدارة التجمع الصحي لتسهيل مهمة جمع البيانات والتأكد من التزام المشاركين بالمشاركة وفق التطوع وحرية الإرادة.

• **أساليب تحليل البيانات:** عقب جمع الاستبانات المسترجعة والتحقق من اكتمالها، تم ترميز البيانات إلكترونياً وإدخالها في برنامج حاسوبي للتحليل الإحصائي (مثل برنامج SPSS). تشمل خطة التحليل الإحصائي عدة مستويات: التحليل الوصفي (Descriptive Analysis) الذي يضمن حساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لإعطاء صورة عامة عن خصائص العينة وتوزيع الإجابات على كل سؤال ومجال من مجالات الدراسة. بعد ذلك يتم الانتقال إلى التحليل الاستدلالي (Inferential Analysis) لاختبار فرضيات الدراسة، حيث ستستخدم اختبارات إحصائية ملائمة لطبيعة كل فرضية: فمثلاً، لاختبار ما إذا كانت الممارسات الحالية فعالة بشكل ملحوظ قد يتم استخدام اختبار t لعينة واحدة لمقارنة متوسط تقييمات المشاركين لمستوى الفعالية بمتوسط افتراضي (يمثل الحد المقبول من الفعالية). كما يمكن استخدام اختبار معامل الارتباط بيرسون لقياس العلاقة بين مستوى تطبيق الممارسات الأمنية (كمتغير مستقل) وبين معدل حوادث الأمن السيبراني أو مستوى انقطاع الخدمة (كمتغير تابع)، وذلك للتحقق من وجود علاقة ذات دلالة إحصائية بينهما. وسيتم استخدام اختبارات الفروق (مثل اختبارات العينات المستقلة أو تحليل التباين الأحادي $ANOVA$) لمعرفة ما إذا كان هناك فروق ذات دلالة في آراء المشاركين أو النتائج بحسب تلك التصنيفات. وستجرى عملية التحليل وفق مستوى دلالة إحصائية (0.05)، وأي نتائج ذات قيمة/احتمالية (P -value) أقل من هذا المستوى تعتبر ذات دلالة إحصائية.

• **الاعتبارات الأخلاقية:** تلتزم الدراسة بأخلاقيات البحث العلمي في جميع مراحلها. فقبل جمع البيانات تم الحصول على موافقة مستنيرة من المشاركين، حيث تم شرح أهداف الدراسة وضمن الحفاظ على سرية معلوماتهم الشخصية وخصوصية إجاباتهم. كما تم حفظ البيانات المجمعة بشكل آمن وعدم استخدامها إلا لأغراض البحث. وبما أن الدراسة تجرى في إطار تجمع صحي رسمي، فقد تم التنسيق مع الجهات المختصة للحصول على الموافقات المطلوبة وضمن توافق إجراءات البحث مع السياسات واللوائح المعمول بها.

من خلال هذه المنهجية، تسعى الدراسة إلى توفير نتائج موثوقة يمكن الاعتماد عليها في تقييم الواقع الحالي لممارسات إدارة مخاطر الأمن السيبراني في تجمع نجران الصحي. لقد روعي في التصميم المنهجي أن يكون قادراً على الإجابة عن أسئلة الدراسة بدقة واختبار الفرضيات بصورة موضوعية، مما يعزز من مصداقية (Validity) النتائج وإمكانية تعميمها على نطاق أوسع من البيئات المماثلة.

أدوات الدراسة

ارتكزت أدوات الدراسة على الاستبانة (Questionnaire) كأداة رئيسية لجمع البيانات الكمية، وفيما يلي تفصيل لأدوات الدراسة وكيفية تطويرها:

- **الاستبانة:** كما أسلفنا، تعتبر الاستبانة من أكثر أدوات جمع البيانات شيوعاً في الدراسات الوصفية نظراً لقدرتها على الوصول إلى عدد كبير من المبحوثين بجهد وتكلفة معقولة. سيتم تصميم استبانة هذه الدراسة خصيصاً لتغطية محاور البحث الأساسية. بحيث تتضمن عدة أقسام: القسم الأول مخصص للمعلومات الديموغرافية والمهنية للمشارك (مثل المسمى الوظيفي، عدد سنوات الخبرة، القسم أو الإدارة). تهدف هذه المعلومات إلى وصف خصائص العينة وربط الاستجابات بخلفيات المشاركين. أما القسم الثاني فسيشمل عبارات تقييمية حول ممارسات إدارة المخاطر السيبرانية المطبقة في التجمع الصحي. وسيتم تقسيم هذا القسم إلى محاور فرعية تعكس عناصر أمن المعلومات: محور السياسات والإجراءات (مثل وجود سياسة أمن معلومات معتمدة وتطبيقها بانتظام)، محور التقنيات والبنية التحتية (مثل توفر جدار ناري، أنظمة كشف التسلل، التحديث الدوري للأنظمة، واستخدام التشفير)، محور التدريب والوعي (مثل عقد دورات تدريبية منتظمة للموظفين حول أمن المعلومات ومدى التزامهم بإرشادات الحماية)، محور الاستجابة للحوادث والطوارئ (مثل وجود فريق أو خطة معتمدة للاستجابة الفورية للحوادث السيبرانية واختبارها دورياً). كل محور يحتوي على عدد من العبارات التي يقيمها المشارك حسب مقياس ليكرت (1 = ضعيف جداً إلى 5 = قوي جداً أو ما شابه)، بما يوفر قياساً كمياً لمدى توافر وكفاءة كل جانب. سيرفق بالاستبانة رسالة توضيحية تبين هدف الدراسة وأهميتها، وتؤكد على سرية الإجابات، وذلك لتعزيز الثقة وتشجيع المشاركة الصادقة.

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 البيانات 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 بيئة نجران الصحية.

(3) الحدود الزمانية (Time Frame): يتم إجراء الدراسة خلال الربع الثالث 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 جعل بعض الجهات أو الأفراد متحفظين في مناقشة التفاصيل الدقيقة للحوادث أو الثغرات لأسباب مفهومة تتعلق بالسرية وحماية السمعة المؤسسية. حاول الباحث 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 بتقاطع المعلومات من مصادر متعددة لزيادة موثوقية الاستنتاجات. من المحددات الأخرى نقص البحوث المحلية السابقة في مجال الأمن السيبراني الصحي بالملكة، 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.

- 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>
- 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>
- 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>
- 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>
- 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*.

- 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>
- 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>
- 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>
- Riggi, J. (2023). *The importance of cybersecurity in protecting patient safety* | Cybersecurity | Center | AHA. <https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety>
- 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>
- 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>
- عفيفي, آ. أ. ع. م. (2024). تأثير تطبيق إدارة المخاطر على مشاريع الرعاية الصحية: دراسة تطبيقية. *المجلة الدولية للبحوث العلمية*, 3(8), 860–892. <https://doi.org/10.59992/IJSR.2024.V3N8P24>