

لمقرر قضايا بحثية ١

الباحث/عبدالسلام العتيبي

الأسبوع السابع



قضايا بحثية ١

Mitigating Cybersecurity Risks in the U.S. Healthcare Sector

إعداد
الباحث/عبدالسلام العتيبي

يعد قطاع الرعاية الصحية في الولايات المتحدة أحد القطاعات الحيوية التي تؤثر بشكل كبير على حياة الأفراد والمجتمعات، وهو يشهد تطورًا مستمرًا في استخدام التكنولوجيا الرقمية. ومع تزايد الاعتماد على الأنظمة الإلكترونية في معالجة البيانات الصحية، يزداد أيضًا تعرض هذا القطاع لمخاطر الأمن السيبراني. هذه المخاطر تهدد ليس فقط خصوصية المرضى وحمايتهم، بل تمتد أيضًا لتؤثر على سلامة النظام الصحي ككل، بما في ذلك تعطيل الخدمات الطبية أو التلاعب بالبيانات الحيوية.

تشمل التهديدات السيبرانية في القطاع الصحي الهجمات مثل البرمجيات الخبيثة، والهجمات الإلكترونية على الشبكات، والاختراقات التي تهدد أمن البيانات الشخصية والحساسة للمرضى. وفي ظل هذا التزايد في المخاطر، أصبح من الضروري تطوير استراتيجيات فعالة لتقليل هذه التهديدات وحماية البيانات والأنظمة الصحية من الهجمات الإلكترونية.

يتناول هذا البحث السبل المختلفة التي يمكن من خلالها تقليل المخاطر السيبرانية في قطاع الرعاية الصحية الأمريكي. سيتم التركيز على الأساليب الوقائية، والتكنولوجيا الحديثة، وكذلك السياسات الحكومية والتنظيمية التي تسعى لضمان بيئة صحية آمنة وخالية من المخاطر السيبرانية.

تتمثل مشكلة هذا البحث في تزايد التهديدات السيبرانية التي تستهدف القطاع الصحي في الولايات المتحدة، مما يعرض بيانات المرضى وخصوصيتهم، وكذلك استمرارية الخدمات الطبية، لخطر حقيقي. على الرغم من التحسينات التكنولوجية الكبيرة في النظام الصحي، إلا أن الهجمات الإلكترونية على المستشفيات، العيادات، ومقدمي الرعاية الصحية أصبحت أكثر تطوراً وتهديداً.

تتمثل الصعوبة الرئيسية في أن العديد من المؤسسات الصحية، سواء الكبيرة أو الصغيرة، تواجه تحديات في تنفيذ تدابير فعّالة لمواجهة هذه المخاطر. قد يكون ذلك نتيجة لعدم توفر الموارد الكافية، نقص الخبرات التقنية، أو حتى ضعف التنسيق بين الجهات الحكومية والقطاع الخاص في التعامل مع التهديدات السيبرانية. إضافة إلى ذلك، تزداد تعقيد المشكلة بسبب التنوع الكبير في الأنظمة التقنية المستخدمة في المؤسسات الصحية، والاختلافات في مستوى الوعي الأمني لدى الموظفين، ما يجعل من الصعب وضع حلول شاملة وفعّالة لحماية النظام الصحي بأكمله.

لذلك، تبرز الحاجة إلى دراسة العوامل المؤدية إلى ضعف الأمان السيبراني في القطاع الصحي، واستخلاص استراتيجيات مبتكرة وفعّالة لمواجهة هذه التهديدات، وضمان توفير بيئة آمنة وسليمة للبيانات الصحية والمعلومات الشخصية للمرضى.

يظهر أن هذا البحث يعد ذا أهمية بالغة في تعزيز فهم التحديات الأمنية التي تواجه القطاع الصحي الأمريكي، وفي تطوير حلول استراتيجية تساهم في الحفاظ على أمان الأنظمة الصحية وحماية بيانات المرضى. تكمن أهمية هذا البحث في النقاط التالية:

١. **حماية بيانات المرضى:** يُعتبر حماية البيانات الصحية للمريض من أهم أولويات القطاع الصحي. الهجمات الإلكترونية قد تؤدي إلى تسريب أو التلاعب بهذه البيانات، مما يعرض خصوصية المرضى للخطر ويؤثر على سمعة المؤسسات الصحية. من خلال هذا البحث، يمكن فهم أفضل الطرق لحماية هذه البيانات وضمان سرّيتها وسلامتها.
٢. **ضمان استمرارية الخدمات الصحية:** الهجمات السيبرانية يمكن أن تعطل أنظمة الرعاية الصحية، مما قد يؤثر بشكل مباشر على تقديم الخدمات الطبية. على سبيل المثال، قد تؤدي الهجمات إلى تعطيل الأنظمة التي تدير السجلات الطبية الإلكترونية أو تلك المسؤولة عن التشخيص والعلاج. البحث يساعد في تطوير استراتيجيات لتقليل المخاطر وضمان استمرارية العمل دون انقطاع.
٣. **تحقيق التوازن بين التكنولوجيا والأمان:** في الوقت الذي تشهد فيه أنظمة الرعاية الصحية تطورًا تكنولوجيًا كبيرًا، تصبح الحاجة ملحة لتطبيق حلول أمنية فعّالة. البحث يساهم في تحديد أفضل الممارسات والتقنيات الحديثة التي يمكن أن توازن بين استخدام التكنولوجيا بشكل فعال وبين حماية الأنظمة من التهديدات السيبرانية.
٤. **مواكبة التهديدات المتطورة:** تتطور الهجمات الإلكترونية باستمرار، ويصعب التنبؤ بكل الأنماط والطرق التي قد يستخدمها القراصنة. من خلال هذا البحث، يتم تقديم تحليل معمق لأحدث التهديدات السيبرانية وكيفية مواجهتها، مما يساهم في تعزيز قدرة المؤسسات الصحية على التكيف مع التغيرات المتسارعة في مشهد الأمان السيبراني.
٥. **التأثير على السياسات والتشريعات الصحية:** يعد البحث بمثابة مرجع مهم لصانعي السياسات في القطاع الصحي والحكومات، حيث يقدم لهم رؤى استراتيجية تساعد في تطوير تشريعات وقوانين تساهم في تعزيز الأمان السيبراني في المؤسسات الصحية. كما يسلط الضوء على أهمية التعاون بين القطاعين العام والخاص لمكافحة التهديدات السيبرانية.

يهدف هذا البحث إلى تحقيق عدة أهداف رئيسية تساهم في تعزيز الأمان السيبراني في قطاع الرعاية الصحية الأمريكي، وتشمل الأهداف التالية:

١. تحليل التهديدات السيبرانية في القطاع الصحي: دراسة الأنواع المختلفة من الهجمات السيبرانية التي تستهدف المؤسسات الصحية، مثل البرمجيات الخبيثة (Malware)، وهجمات طلب الفدية (Ransomware)، والاختراقات الأمنية (Data Breaches).
٢. استكشاف التحديات التي تواجه المؤسسات الصحية في حماية بيانات المرضى: تحديد العوامل التي تسهم في ضعف الأمان السيبراني في المؤسسات الصحية، بما في ذلك قلة الوعي الأمني لدى الموظفين، ضعف البنية التحتية التقنية، وتعدد الأنظمة المستخدمة.
٣. مراجعة الاستراتيجيات الحالية لحماية الأنظمة الصحية: تقييم فعالية هذه الاستراتيجيات وتحديد نقاط الضعف التي يجب معالجتها.
٤. اقتراح حلول وتقنيات مبتكرة لتحسين الأمان السيبراني في القطاع الصحي: دراسة تطبيق الحلول التقنية المختلفة مثل أدوات مراقبة الشبكات وحماية الأنظمة لتقليل المخاطر.
٥. تحليل دور السياسات الحكومية والتشريعات في تعزيز الأمان السيبراني في القطاع الصحي: استكشاف التشريعات والسياسات الحكومية الحالية التي تؤثر في الأمان السيبراني في مجال الرعاية الصحية، مثل قانون "HIPAA" قانون التأمين الصحي القابل للنقل والمساءلة.
٦. زيادة الوعي الأمني لدى العاملين في القطاع الصحي: تحديد الطرق الفعالة التي يمكن من خلالها تعزيز الوعي الأمني والتدريب المستمر للموظفين داخل المؤسسات الصحية، لتقليل الأخطاء البشرية التي قد تؤدي إلى اختراقات أمنية.
٧. تحليل الفجوات في البحث الأكاديمي والممارسات العملية: دراسة الفجوات بين البحث الأكاديمي والممارسات العملية في مجال الأمان السيبراني للقطاع الصحي، وتحديد المجالات التي تحتاج إلى مزيد من البحث والابتكار.

الأمن السيبراني: (Cybersecurity) مفهوم الأمن السيبراني هو حماية الأنظمة الإلكترونية والشبكات من الهجمات أو الاختراقات. في سياق القطاع الصحي، يشمل ذلك حماية البيانات الطبية الحساسة، ضمان استمرارية الأنظمة الصحية، وتأمين عملية نقل البيانات بين مقدمي الرعاية الصحية.

التهديدات السيبرانية: (Cyber Threats) يشمل هذا المفهوم الأنواع المختلفة من الهجمات التي يمكن أن تستهدف المؤسسات الصحية، مثل الفيروسات والبرمجيات الخبيثة، هجمات طلب الفدية (Ransomware)، والهجمات على قواعد البيانات. يشمل أيضًا التهديدات الداخلية التي قد تحدث نتيجة لأخطاء بشرية أو سوء إدارة.

حماية البيانات الصحية: (Health Data Protection) حماية المعلومات الطبية الحساسة للمرضى من الوصول غير المصرح به أو التلاعب بها. يشمل هذا المفهوم التدابير التي يجب أن تتخذها المؤسسات الصحية لضمان سلامة هذه البيانات طوال فترة استخدامها، سواء أثناء تخزينها أو نقلها.

التشفير: (Encryption) التشفير هو عملية تحويل البيانات إلى صيغة لا يمكن قراءتها إلا من قبل الأشخاص المصرح لهم بذلك. يعتبر من أكثر الوسائل فعالية لضمان حماية البيانات الصحية أثناء النقل أو التخزين.

الأنظمة الصحية الإلكترونية: (Electronic Health Systems) تشمل الأنظمة المستخدمة لتخزين وتبادل البيانات الطبية، مثل السجلات الصحية الإلكترونية (EHR)، وأنظمة إدارة المستشفيات، والتي أصبحت عرضة للتهديدات السيبرانية بسبب استخدامها الواسع وانتشارها.

الامتثال والتشريعات: (Compliance and Regulations) يشمل الامتثال للقوانين والتشريعات التي تفرض على المؤسسات الصحية اتباع معايير معينة لحماية بيانات المرضى، مثل قانون HIPAA (قانون التأمين الصحي القابل للنقل والمساءلة) في الولايات المتحدة، والذي يحدد معايير حماية المعلومات الصحية الشخصية.

الوعي الأمني والتدريب: (Security Awareness and Training) مفهوم يتعلق بتعليم وتدريب الموظفين على أفضل ممارسات الأمان السيبراني لتقليل الأخطاء البشرية وتحسين الدفاعات الأمنية في المؤسسات الصحية.

دراسات حول تأثير الهجمات السيبرانية على القطاع الصحي:

- العديد من الدراسات أظهرت أن الهجمات السيبرانية، مثل هجمات الفدية (Ransomware)، أصبحت تهديدًا متزايدًا للقطاع الصحي. دراسة **Pothier et al. (2020)** أظهرت أن المستشفيات أصبحت أكثر عرضة للهجمات بسبب الأنظمة القديمة وعدم تحديث البرمجيات.
- **Zhou et al. (2019)** تحدثوا عن تأثير هجمات الفدية على المستشفيات، حيث أظهرت دراستهم أن هذه الهجمات تؤدي إلى تعطيل خدمات الرعاية الصحية وتسبب في تأخير في تقديم العلاج للمرضى.

دراسات حول أطر السياسات والتشريعات في حماية البيانات الصحية:

- دراسة **Lustgarten et al. (2018)** استعرضت القوانين المتعلقة بحماية البيانات في القطاع الصحي، مثل **HIPAA**، وناقشت التحديات المتعلقة بتنفيذ هذه القوانين في ظل تزايد استخدام التقنيات الحديثة في مجال الرعاية الصحية.
 - دراسة **Choi et al. (2021)** تناولت الدور الذي تلعبه اللوائح الحكومية في تعزيز الأمان السيبراني في المستشفيات وكيف يمكن تحسين التشريعات لمواكبة التطورات التكنولوجية.
- ### دراسات حول أفضل الممارسات والأنظمة الوقائية:
- **Gartner (2022)** أظهرت دراسة حديثة حول "أفضل ممارسات الأمان السيبراني في القطاع الصحي"، وأكدت على أهمية استخدام أدوات الذكاء الاصطناعي والتحليلات المتقدمة لمراقبة الشبكات والكشف المبكر عن الأنشطة غير الطبيعية.
 - **Hollis et al. (2020)** ركزوا على استراتيجيات الوقاية، مشيرين إلى أن المؤسسات الصحية التي تعتمد على التشفير المتقدم والتدابير الأمنية متعددة الطبقات تكون أكثر قدرة على التصدي للتهديدات السيبرانية.

دراسات حول التحديات التي تواجه المؤسسات الصحية الصغيرة: العديد من الدراسات تسلط الضوء على الفجوات الأمنية في المؤسسات الصحية الصغيرة، مثل دراسة **Harris et al. (2019)** التي أشارت إلى أن المستشفيات الصغيرة تعاني من نقص في الموارد المالية والموارد البشرية المتخصصة في الأمن السيبراني، ما يجعلها أكثر عرضة للهجمات الإلكترونية.

دراسات حول التدريب والوعي الأمني: دراسة **Shah et al. (2018)** تناولت أهمية الوعي الأمني والتدريب المستمر للعاملين في القطاع الصحي، موضحة أن الموظفين الذين يتم تدريبهم على ممارسات الأمان السيبراني هم أقل عرضة لارتكاب الأخطاء التي قد تؤدي إلى اختراقات أمنية.

مقدمة: في ظل التزايد المستمر في استخدام التقنيات الرقمية والتكنولوجيا الحديثة في القطاع الصحي، أصبح الأمان السيبراني أحد أبرز القضايا التي تواجه المؤسسات الصحية في الولايات المتحدة. إن حماية البيانات الصحية الشخصية، وهي من أكثر أنواع البيانات حساسية، أصبح أمرًا حيويًا،

اعتمد على منهجية دراسة متعدد الأبعاد يتضمن عدة جوانب تحليلية وتقنية وتقييمية لفهم المخاطر السيبرانية في القطاع الصحي . يمكن تلخيص المنهجية المستخدمة في الدراسة على النحو التالي:

منهجية التحليلي: (Analytical Model) يعتمد الباحث في دراسته على تحليل التهديدات السيبرانية التي تواجه القطاع الصحي، مما يتطلب دراسة الأنواع المختلفة للهجمات السيبرانية مثل هجمات الفدية، البرمجيات الخبيثة، وخرق البيانات.

منهجية الوصفي: (Descriptive Model) يهدف الباحث إلى وصف واقع الأمان السيبراني في القطاع الصحي الأمريكي، من خلال مراجعة الأدبيات الحالية، والممارسات الأمنية المعتمدة في المؤسسات الصحية.

منهجية المقارن: (Comparative Model) قد يعتمد الباحث على مقارنة المؤسسات الصحية المختلفة من حيث حجمها ومواردها المالية والبشرية، وكذلك نوعية التقنيات الأمنية المستخدمة. على سبيل المثال، يمكن مقارنة الأمان السيبراني في المستشفيات الكبيرة (التي تمتلك موارد تقنية ضخمة) مع المستشفيات الصغيرة أو العيادات (التي قد تفتقر إلى نفس الموارد).

النموذج التقييمي: (Evaluative Model) يتناول الباحث تقييم فعالية الاستراتيجيات الأمنية الحالية التي تتبناها المؤسسات الصحية، مثل استخدام تقنيات التشفير لحماية البيانات الصحية.

منهجية التوجيهي (Prescriptive Model) هذا النموذج يهدف إلى تقديم حلول واستراتيجيات للتعامل مع المخاطر السيبرانية في القطاع الصحي. من خلال تحليل التهديدات والحلول الحالية، يقدم الباحث توصيات للتقنيات والاستراتيجيات التي يجب أن تتبناها المؤسسات الصحية لتعزيز أمانها السيبراني.

منهجية الوقائي: (Preventive Model) يعتمد الباحث على فحص الإجراءات الوقائية التي يجب على المؤسسات الصحية اتخاذها لمنع الهجمات السيبرانية من البداية.

المنهجية التنظيمي: (Organizational Model) يهدف هذا النموذج إلى دراسة الهيكل التنظيمي داخل المؤسسات الصحية وتأثيره على الأمان السيبراني. على سبيل المثال، يمكن فحص دور الفرق الأمنية داخل المؤسسات الصحية وكيفية تنسيقها مع إدارات تكنولوجيا المعلومات والموارد البشرية لضمان تنفيذ سياسات الأمان بشكل فعال.

يعتمد على مجموعة من الأدوات الإحصائية لفهم المخاطر الحالية، تقييم فعالية التدابير الحالية، وتقديم توصيات قابلة للتنفيذ.

جمع البيانات (Data Collection) تقارير حول الحوادث الأمنية المتعلقة بالرعاية الصحية واستبيانات من المتخصصين في الأمن السيبراني في المؤسسات الصحية ودراسات حالة حول الهجمات السيبرانية (مثل الهجمات بواسطة برامج الفدية).

التحليل الوصفي: (Descriptive Analysis) يمكن استخدام التحليل الوصفي لفهم توزيع الحوادث السيبرانية في القطاع الصحي. على سبيل المثال، يمكن حساب المتوسط والانحراف المعياري لعدد الحوادث سنوياً عبر مختلف المستشفيات والعيادات.

التحليل الانحداري (Regression Analysis) يمكن استخدام التحليل الانحداري لفهم العلاقة بين العوامل المختلفة وتأثيرها على خطر الهجمات السيبرانية في القطاع الصحي. على سبيل المثال:

اختبار الفرضيات (Hypothesis Testing) ، قد تكون الفرضية هي أن "المؤسسات الصحية التي تطبق برامج تدريبية منتظمة على الأمن السيبراني لديها نسبة أقل من الهجمات السيبرانية مقارنة بتلك التي لا تطبقها."

التحليل الشبكي (Network Analysis) نظراً لأن قطاع الرعاية الصحية يتضمن العديد من الأطراف المتداخلة مثل المستشفيات، مزودي الخدمات، الشركات التقنية، والوكالات الحكومية، يمكن استخدام التحليل الشبكي لفحص الروابط بين هذه الأطراف وتأثيرها على انتشار الهجمات السيبرانية.

تحديد المخاطر والتوقعات (Risk Identification and Forecasting) باستخدام نماذج التنبؤ مثل النماذج الزمنية (Time Series Analysis)، يمكن توقع عدد الحوادث السيبرانية المستقبلية في القطاع الصحي بناءً على البيانات التاريخية.

التحليل المتقدم: التعلم الآلي (Machine Learning) يمكن استخدام تقنيات التعلم الآلي لتحليل الأنماط في الهجمات السيبرانية. على سبيل المثال، يمكن تدريب نماذج تصنيف (مثل أشجار القرار أو الشبكات العصبية) للتنبؤ بأنواع الهجمات السيبرانية الأكثر احتمالاً بناءً على

يستطيع الباحث تقديم تحليلات مستندة إلى أسس علمية وتقنية وواقعية، تساهم في تطوير استراتيجيات فعّالة لحماية القطاع الصحي من المخاطر السيبرانية. **الاستنتاجات والنتائج:** أظهرت الدراسات أن هناك فجوة كبيرة بين التطبيقات التقنية المتاحة والأمن الفعلي في القطاع الصحي. تحتاج المؤسسات الصحية إلى تبني استراتيجيات أمان سيبراني متعددة الطبقات تشمل التقنيات الحديثة، ورفع الوعي الأمني، وتعزيز الامتثال للتشريعات الحكومية لحماية البيانات الصحية.

التوصيات التي بناءً عليها استند الباحث في دراسته: تركز توصيات البحث على ضرورة تحسين التعاون بين القطاعين العام والخاص لتطوير حلول أمنية فعّالة، إضافة إلى تحسين السياسات الحكومية وتحفيز التدريب المستمر للعاملين في القطاع الصحي.



Thank You