

مهارات بحثية ١

الباحث/عبدالسلام العتيبي

الأسبوع السابع



مهارات بحثية ١

Mitigating Cybersecurity Risks in the U.S. Healthcare Sector

إعداد
الباحث/عبدالسلام العتيبي

يعتبر القطاع الصحي أحد أكثر القطاعات الحيوية في أي دولة، حيث يتعامل مع بيانات شخصية وحساسة تتعلق بصحة الأفراد. ومع تزايد الاعتماد على التكنولوجيا الرقمية في إدارة السجلات الطبية، والأنظمة الصحية الإلكترونية، والخدمات الصحية عن بُعد، أصبح القطاع الصحي في الولايات المتحدة هدفًا متزايدًا للهجمات السيبرانية. إن الأمن السيبراني في هذا القطاع يمثل تحديًا كبيرًا، نظرًا للطبيعة الحساسة للبيانات الصحية وحجم المعلومات التي يتم تداولها عبر الشبكات الإلكترونية.

في السنوات الأخيرة، شهد القطاع الصحي في الولايات المتحدة العديد من الحوادث الأمنية التي أثرت بشكل سلبي على قدرة المؤسسات الصحية في تقديم الرعاية الطبية، وشهدنا العديد من الاختراقات التي تسببت في تسريب معلومات حساسة للمرضى أو تعطيل الأنظمة الصحية بشكل كامل. على سبيل المثال، شهدت العديد من المستشفيات في الولايات المتحدة هجمات فدية (Ransomware) استهدفت أنظمتها الإلكترونية، مما أسفر عن تأخير في تقديم العلاج وتوقف الأنظمة الحيوية. كما تزايدت حوادث تسريب البيانات نتيجة للاختراقات الإلكترونية، مما عرض معلومات المرضى الشخصية للخطر.

تسعى هذه الدراسة إلى تقديم تحليل شامل للمخاطر السيبرانية التي تهدد القطاع الصحي في الولايات المتحدة، مع التركيز على تحديد الأسباب الرئيسية لهذه المخاطر، وفحص الاستراتيجيات الحالية المستخدمة في حماية البيانات الصحية. كما تهدف الدراسة إلى اقتراح حلول عملية ومبنية على الأدلة للحد من المخاطر السيبرانية، بما في ذلك تطبيق تقنيات جديدة مثل الذكاء الاصطناعي، وتدابير الوقاية المستمرة، وتوفير التدريب المستمر للعاملين في هذا القطاع ومن خلال هذه الدراسة، سيتم تسليط الضوء على أهمية تعزيز الأمن السيبراني في المؤسسات الصحية، وتقديم توصيات استراتيجية لتحسين مستوى الأمان وحماية البيانات الصحية. كما تهدف الدراسة إلى تحفيز التحسينات في السياسات الأمنية الخاصة بالمؤسسات الصحية في الولايات المتحدة، وزيادة الوعي بالأهمية المتزايدة لأمن المعلومات في هذا القطاع الحساس.

عينة الغرض: (Purposeful or Judgmental Sampling) يعتمد الباحث هنا على اختيار أفراد أو مؤسسات معينة من القطاع الصحي بناءً على خصائص معينة أو معايير ذات صلة بالبحث. يتم اختيار المؤسسات الصحية التي تعاني من مشكلات أمنية سيبرانية أو التي تعرضت لهجمات إلكترونية كبيرة، أو التي تملك تجربة غنية في مواجهة هذه التهديدات.

• **مثال:** قد يختار الباحث مستشفيات تعرضت لهجوم فدية (Ransomware) أو عيادات تتمتع بتطبيقات تقنية حديثة للأمن السيبراني، مما يساعد في تقييم فعالية الإجراءات المتخذة.

عينة المقابلات المتعمقة: (In-depth Interview Sampling) في هذه الحالة، قد يختار الباحث خبراء في مجال الأمن السيبراني، مثل مديري أمن المعلومات، وموظفي تكنولوجيا المعلومات، أو القائمين على حماية البيانات في المستشفيات والعيادات.

• **مثال:** مقابلة مع مسؤولين في المستشفيات الكبرى والصغيرة، لمناقشة تقنيات الأمان المتبعة ومدى فعاليتها.

عينة الحوادث الأمنية: (Incident-Based Sampling) قد يقوم الباحث بجمع البيانات من تقارير الحوادث الأمنية الصادرة عن المؤسسات الصحية بعد تعرضها للاختراقات. في هذا السياق، يمكنه اختيار المؤسسات التي تعرضت لهجمات سيبرانية أو تسريبات بيانات في فترة زمنية محددة لدراسة تأثير هذه الحوادث وتقييم الإجراءات الأمنية المتخذة.

• **مثال:** اختيار عينة من المستشفيات التي تعرضت لهجوم فدية وتوثيق استجابتها لهذه الحوادث.

عينة مقارنة: (Comparative Sampling) في بعض الحالات، قد يختار الباحث مقارنة المؤسسات الصحية التي تتمتع بموارد كبيرة (مثل المستشفيات الأكاديمية الكبيرة) مع تلك التي تملك موارد محدودة (مثل العيادات الصغيرة أو المستشفيات الإقليمية).

استخدام الأسلوب الإحصائي لتحديد حجم العينة. يتم هذا عادة باستخدام الصيغ الإحصائية الخاصة بحساب حجم العينة.
الصيغة الأساسية لتحديد حجم العينة:
لحساب حجم العينة بطريقة إحصائية، يمكن استخدام الصيغة التالية:

$$\frac{Z^2 \times p \times (1 - p)}{E^2} = n$$

n: حجم العينة المطلوب

z: القيمة الحرجة (Critical Value) المرتبطة بمستوى الثقة

p: التقدير المبدئي للنسبة المئوية للظاهرة المدروسة

E: هامش الخطأ المقبول



Thank You