

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص إدارة المخاطر



عنوان البحث

نموذج مقترح لإدارة مخاطر الأمن السيبراني في شركات التأمين

بالتطبيق على

قطاع التأمين بالمملكة العربية السعودية

إعداد الطالب/ عبدالله أحمد الجنيد

إشراف/

العام الدراسي:

٢٠٢٥م

مقدمة:

نعيش اليوم في خضم مجتمع المعرفة والتدفق المعلوماتي الذي ساهم بشكل كبير في غزارة ووفرة معلوماتية غير مسبوقة أفضت إلى ظاهرة الانفجار المعلوماتي بما له وما عليه من إيجابيات وسلبيات على المجتمع الدولي بكافة مؤسساته وأنشطته الاقتصادية، كما تسبب من جهة أخرى في مشكلات أمنية ومالية كثيرة متفاوتة الخطورة والضرر على تلك المؤسسات، مما تولد عنها نوع جديد من المخاطر والتهديدات بما يعرف بالمخاطر السيبرانية، والتي استدعت في كثير من الحالات وضع استراتيجيات أمنية معقدة للتدخل المناسب لحماية البيانات والمعلومات الشخصية والمشاركة وهو ما يطلق عليه بالأمن السيبراني. وتعد المخاطر السيبرانية من المخاطر وليدة العصر والتي تؤثر على أنشطة العديد من المؤسسات الاقتصادية بمختلف أنواعها ومن ثم على الاقتصاد العالمي. وفي ضوء التطورات الجديدة والمتسارعة في تقنيات الأعمال اكتسب الأمن السيبراني المزيد من الاهتمام بين الباحثين نتيجةً للتوسع في طرق ووسائل مبيعات مختلف السلع والخدمات عبر شبكة الإنترنت في جميع أنحاء العالم، وارتفاع العمل عن بعد والجرائم السيبرانية الأخيرة (Smaili et al., 2022).

وأصبح المجتمع معتمداً بشكل كبير على التقنيات التكنولوجية وقواعد البيانات والمعلومات، ومن ثم أصبحت المخاطر السيبرانية أحد أكبر التهديدات للإنجاز الاستراتيجي للعديد من المؤسسات الاقتصادية (Foglietta et al., 2018). فالدور الرئيسي لقواعد البيانات والمعلومات في المجتمعات المعاصرة جعلها محل استهداف وتهديد يستدعي تأمينها وحمايتها من كافة الجرائم التي تواجهها، حيث تعمل الهجمات السيبرانية على وقوع أضراراً كبيرة حتى مع الشركات الأكثر تطوراً، وعادة ما يؤثر على سمعتها بين العملاء وعلى قيمتها السوقية مما يؤدي إلى ارتفاع التكاليف المستقبلية الناتجة عن الهجوم السيبراني ومن ثم يستوجب منها إجراء تحولات استراتيجية في سياساتها المستقبلية لتقليل الأضرار المحتملة الناتجة عن الهجوم السيبراني (Kamiya et al., 2021).

وهناك العديد من المخاطر التي تهدد صناعة التأمين، وتتمثل هذه المخاطر في إمكانية توافر مجموعة من العوامل بصورة تؤدي إلى نتائج غير مرغوب فيها، هذه العوامل قد تتعلق بالمخاطر المرتبطة بالاكنتاب والسيولة وأخطار ناتجة عن العوامل الاجتماعية التي تمارس فيها هذه الشركة نشاطها كالإهمال والشرقة، لذا تعتمد هذه الشركات على استراتيجيات وطرق محددة للتقليل من المخاطر والمحافظة على استمرارية وتنافسية هذه الشركات.

وتعتبر شركات التأمين شأن باقي المؤسسات الاقتصادية، حيث إنها تتعامل مع العديد من العملاء من مختلف شرائح المجتمع مما يراكم لديها كم هائل من البيانات والمعلومات التي تتعلق بعملائها، وأنشطتها الخدمية من حصيلة الأقساط والمطالبات والتسويات وغيرها من البيانات والمعلومات التي يتطلب بقاء الشركة في السوق الحالي أو المستقبلي الحفاظ على سريتها وسلامتها من الهجمات السيبرانية.

مشكلة الدراسة:

لقد باتت الهجمات السيبرانية وانتهاكات البيانات والمعلومات تستنزف معظم المؤسسات الاقتصادية والدول بشكل فاق تأثير الصراعات والحروب حول العالم، حيث أن أسواق الأمن السيبراني تشهد نمواً غير مسبوق في ظل تزايد التهديدات الإلكترونية، والحاجة الملحة إلى حماية البيانات والبنية التحتية الرقمية لمختلف المؤسسات، وخلال السنوات الأخيرة أصبح الأمن السيبراني جزءاً لا يتجزأ من استراتيجيات الحكومات وكافة الشركات الكبرى على مستوى العالم. حيث تُعد المخاطر السيبرانية من التحديات الرئيسية التي تواجه قطاع التأمين في المملكة العربية السعودية، نظراً لتزايد حوادث الاختراقات السيبرانية والتهديدات الرقمية بشكل ملحوظ في السنوات الأخيرة. رغم التطورات التكنولوجية المتسارعة، لا تزال العديد من شركات التأمين تعاني من ضعف في استراتيجيات إدارة المخاطر السيبرانية، مما يؤدي إلى فقدان البيانات، وتعطيل العمليات، وتضرر سمعة الشركات. تتجلى مشكلة البحث في عدم وجود نموذج متكامل ومناسب لإدارة مخاطر الأمن السيبراني يتماشى مع الخصوصيات الثقافية والتنظيمية لقطاع التأمين في المملكة. بالإضافة إلى ذلك، هناك نقص في الوعي والمعرفة بين الموظفين حول أهمية الأمن السيبراني، مما يزيد من تعرض الشركات للمخاطر. لذا، يسعى هذا البحث إلى تطوير نموذج مقترح لإدارة مخاطر الأمن السيبراني، يتضمن استراتيجيات فعالة وممارسات أفضل، ويأخذ في الاعتبار البيئة المحلية والتحديات الخاصة بقطاع التأمين في المملكة. من خلال هذا النموذج.

أهمية الدراسة:

تأتي أهمية البحث من منطلق ما تشكله المخاطر السيبرانية من تهديدات كبيرة على جميع العمليات التشغيلية والأنشطة الخدمية التي تقدمها شركات التأمين، ودور الأمن السيبراني في إدارة تلك التهديدات والمخاطر السيبرانية التي تتعرض لها تلك الشركات. ويمكن تقسيم أهمية الدراسة إلى كل من:-

- الأهمية العلمية:

تساهم الدراسة في إثراء الأدبيات الأكاديمية حول إدارة مخاطر الأمن السيبراني، خاصة في سياق قطاع التأمين في المملكة العربية السعودية، مما يفتح مجالات جديدة للدراسات المستقبلية. كما يوفر البحث نموذجاً مقترحاً لإدارة المخاطر، مما يساهم في تطوير نماذج نظرية جديدة تعزز من فهم التحديات السيبرانية وكيفية إدارتها بشكل فعال. بالإضافة إلى أنه يجمع بين مجالات الأمن السيبراني، التأمين، وإدارة المخاطر، مما يعزز التعاون بين هذه التخصصات ويساهم في تقديم رؤية شاملة حول كيفية التصدي للمخاطر.

- الأهمية العملية:

يوفر النموذج المقترح استراتيجيات فعالة تساهم في تعزيز مستوى الأمان في شركات التأمين، مما يقلل من تعرضها للتهديدات السيبرانية. ومن خلال تحسين إدارة مخاطر الأمن السيبراني، يمكن أن تزداد ثقة العملاء في شركات التأمين، مما يساهم في تعزيز سمعة الشركات وزيادة ولاء العملاء. كما يساهم البحث في دعم الشركات في الامتثال للمتطلبات التنظيمية والقوانين المتعلقة بالأمن السيبراني، مما يقلل من المخاطر القانونية والمالية. ويوفر البحث أدوات

تحليلية تساعد الشركات على تحديد مجالات الاستثمار اللازمة لتعزيز الأمن السيبراني وتحسين العمليات التشغيلية. وأخيراً يساعد البحث في رفع مستوى الوعي بين الموظفين حول أهمية الأمن السيبراني، ويشجع على تطوير برامج تدريبية فعالة لتعزيز المهارات والمعرفة في هذا المجال.

أهداف الدراسة:

تهدف الدراسة إلى تحديد دور الأمن السيبراني في إدارة مخاطر شركات التأمين، ويمكن صياغة هذا الهدف العام في مجموعة من الأهداف الفرعية كالتالي:

- التعرف على المفاهيم المختلفة المرتبطة بموضوع إدارة مخاطر الأمن السيبراني.
- إبراز أهم التحديات التي تواجه شركات التأمين فيما يتعلق بالأمن السيبراني ودوره في إدارة المخاطر السيبرانية بتلك الشركات.
- تحليل وتحديد المخاطر السيبرانية الأكثر شيوعاً التي تواجه شركات التأمين في المملكة العربية السعودية.
- دراسة الوضع الحالي لإدارة مخاطر الأمن السيبراني في قطاع التأمين، بما في ذلك استراتيجيات الإدارة والممارسات المتبعة.
- تصميم نموذج متكامل لإدارة مخاطر الأمن السيبراني يتناسب مع خصوصيات قطاع التأمين في المملكة، مع التركيز على استراتيجيات فعالة للتصدي للمخاطر.

تساؤلات الدراسة

- ١- ما هي المخاطر السيبرانية الأكثر شيوعاً التي تواجه شركات التأمين في المملكة العربية السعودية؟
- ٢- كيف يتم تقييم الوضع الحالي لإدارة مخاطر الأمن السيبراني في قطاع التأمين؟
- ٣- ما هي الاستراتيجيات والممارسات الحالية التي تتبعها شركات التأمين في إدارة المخاطر السيبرانية؟
- ٤- كيف يمكن تصميم نموذج متكامل لإدارة مخاطر الأمن السيبراني يتناسب مع احتياجات شركات التأمين في المملكة؟

فروض الدراسة:

تعتمد الدراسة على فرضية أساسية تشير إلى "وجود علاقة بين إجراءات الأمن السيبراني المطبقة ومستوى إدارة المخاطر السيبرانية بشركات التأمين". ولاحظت صحة هذه الفرضية، تم طرح مجموعة من الفرضيات التي ستخضع للدراسة والتحليل. كما يلي:

- فرضية الدراسة الأولى: هناك علاقة إيجابية بين مستوى الوعي بمخاطر الأمن السيبراني وفعالية إدارة مخاطر الأمن السيبراني في شركات التأمين.
- فرضية الدراسة الثانية: وجود نموذج متكامل لإدارة مخاطر الأمن السيبراني يؤدي إلى تحسين مستوى الأمان وتقليل الحوادث السيبرانية في شركات التأمين.
- الفرضية الدراسة الثالثة: هناك علاقة بين تطبيق برامج التدريب والتوعية على الأمن السيبراني وزيادة كفاءة الموظفين في التصدي للمخاطر السيبرانية.
- الفرضية الدراسة الرابعة: شركات التأمين التي تتبنى استراتيجيات إدارة مخاطر الأمن السيبراني تكون أكثر قدرة على الحفاظ على ثقة العملاء مقارنة بالشركات التي لا تتبنى هذه الاستراتيجيات.

الدراسات السابقة:

يهدف العرض الحالي للدراسات السابقة إلى التعرف على أهم المحاولات والأسس العلمية التي تمت لإدارة المخاطر السيبرانية لشركات التأمين، والتعرف على أهم العقبات التي واجهت الباحثين لبحث هذا الموضوع، وبالتالي الوقوف على أركان الفجوة البحثية التي تنطلق منها الدراسة. ولعل من أهم الدراسات التي تناولت هذا الموضوع دراسة (Shachelford, ٢٠١٢) بعنوان: "Should your firm invest in cyber risk insurance?" إلى تحليل تأثير الهجمات السيبرانية على الشركات، وبعض القوانين الأمريكية المعمول بهاء والتي تشكل استجابات القطاع الخاص لانتهاكات البيانات والمدى الذي يساعد فيه التأمين ضد المخاطر السيبرانية في التخفيف من التهديد السيبراني، وذلك لتعزيز الأمن السيبراني بشكل عام، والمساعدة في تأمين البنية التحتية لتلك الشركات، ومن أهم نتائج الدراسة بأنه لكي تتمكن الشركات من الحد من المخاطر السيبرانية التي تتعرض لها، يتعين عليها أن تكون استباقية وأن تستثمر أولاً في تعزيز أمنها السيبراني، وهذا يشمل تركيب جدران الحماية، وفرض التشفير، والاستثمار في قدرات الكشف عن الاختراقات، وبعد ذلك يتعين على الشركات أن تقيم تغطيتها التأمينية الحالية وأن تجري تحليلاً للتكاليف والفوائد المترتبة على تعرضها للتهديدات والمخاطر السيبرانية.

وأشارت دراسة (Young, D., Lopez, J., Jr, ٢٠١٦) بعنوان "A framework for incorporating insurance in critical infrastructure cyber risk strategies" إلى أن صناعة التأمين استخدمت لسنوات كثيرة التحليلات الكمية لمختلف المخاطر التي تتعرض لها وخاصة المخاطر الناتجة عن تكنولوجيا المعلومات، وذلك بغرض التقليل من الآثار السلبية المترتبة على تحقق تلك المخاطر، ولكن أصبح الآن هناك ضرورة ملحة للبحث عن طرق حديثة لدعم التقييمات الكمية للمخاطر المتعلقة بالإنترنت بهدف تقليل المخاطر السيبرانية التي تتعرض لها مع الحفاظ على حد معين من تكلفة الأمن السيبراني، ولتحقيق تلك الأهداف، تقوم شركات التأمين بتجميع وتحليل البيانات الإحصائية باستمرار لتحسين تنبؤاتها المستقبلية في هذا الشأن، وتحفيز استثمارات العملاء في الحماية الذاتية وتحديث النماذج الإحصائية المستخدمة في عمليات التقييم بشكل دوري لتحسين دقة تقديرات تلك المخاطر، وبالتالي هدفت الدراسة إلى اقتراح إطار علمي يشتمل على المبادئ التشغيلية لصناعة التأمين لتوفير تقديرات كمية مناسبة ودقيقة للمخاطر السيبرانية، مما يتيح إمكانية استخدامها في صياغة استراتيجيات وسياسات جديدة تعالج المخاطر والتهديدات السيبرانية لشركات التأمين، وكذلك اقتراح مستويات الاستثمار المناسبة في الأمن السيبراني.

كما تطرقت دراسة (مروة، ٢٠١٧م) بعنوان " دور نظم المعلومات الإلكترونية في إدارة مخاطر الصناعة التأمينية دراسة حالة عينة من شركات التأمين الجزائرية" إلى التعرف على دور نظم المعلومات الإلكترونية في إدارة مخاطر الصناعة التأمينية، وذلك من خلال دراسة حالة لعينة من شركات التأمين بالجزائر، وخلصت الدراسة إلى مجموعة من النتائج أهمها ظهور مخاطر جديدة نتيجة الطفرة الكبيرة التي وقعت في وسائل الاتصال وشبكات المعلومات، مما يستوجب أخذ كافة التدابير اللازمة والممكنة لحماية أنظمة المعلومات في الشركة وحماية عماله، كما أن نظم المعلومات الإلكترونية تسهم وبشكل فعال في إدارة مختلف المخاطر السيبرانية التي يمكن أن تتعرض لها شركات التأمين، كما أوصت الدراسة على ضرورة التحديث المستمر لنظم المعلومات في الشركة بالنظر إلى أهميته في إدارة المخاطر لا سيما مخاطر الملاءة المالية في شركة التأمين، والعمل على توفير برامج ودورات تدريبية كافية للمستخدمين في مجال المعلوماتية من أجل زيادة فعالية هذه النظم.

وهدفت دراسة (الربيعي، خلود هادي، وآخرون، ٢٠١٧م) بعنوان " أمن وسرية المعلومات وأثرها على الأداء التنافسي : دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية" إلى التعريف بأمن وسرية المعلومات وتبسيط الضوء على الإجراءات اللازمة لأمن وسرية المعلومات وكيفية أداء أقسام شركات التأمين لها، ومعرفة ما إذا كان هناك تأثير لاثمن وسرية المعلومات على الأداء التنافسي لشركات التأمين، وطبقت الدراسة على شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي باستخدام أداة الاستبيان لجمع البيانات من عدد من موظفي كان الشركتين، ومن أهم نتائج الدراسة أن هناك انخفاض في الوعي بأمن المعلومات وسريتها في شركات التأمين وعدم تطبيق طرق الحماية المتبعة في أغلب شركات العالم، كما بينت الدراسة وجود علاقة ارتباط وتأثير بين أمن وسرية المعلومات والأداء التنافسي لشركات التأمين قيد البحث.

أما دراسة (Talish, S.A.,2018) فقد ركزت على أن اختراق البيانات والمخاطر الإلكترونية يشكل تهديدات رئيسية تواجه معظم المؤسسات، وتشير الدراسات إلى أن معظم المؤسسات لا تتمتع بالحماية الأمنية الكافية والتعامل مع الهجمات السيبرانية التي تلحق بالبيانات والمعلومات والالتزام لقوانين الخصوصية، وقد بينت الدراسة كيف تلعب شركات التأمين دوراً حاسماً في مساعدة مختلف المؤسسات في الالتزام لقوانين الخصوصية، والتعامل مع مختلف الهجمات الإلكترونية، كما تناولت تحليل ودراسة محتوى دليل شركات التأمين وخدمات إدارة المخاطر الإلكترونية التي تلحق بشركات التأمين، وسلطت الضوء على كيفية عمل شركات التأمين مع تهديدات الأمن السيبراني بعيداً عن تجميع ونقل المخاطر، وكيفية تقديم شركات التأمين تأميناً إلكترونياً وخدمات إدارة مخاطر فريد ومتطورة بما يتناسب مع المخاطر الحديثة نتيجة التعامل مع الكم الهائل من البيانات والمعلومات في شركات التأمين.

وقدمت دراسة زايد وآخرون، ٢٠١٩م بعنوان " التأمين الرقمي دراسة تطبيقية على قطاع التأمين السعودي " تحليلاً حول التحول الرقمي في قطاع التأمين بشركات التأمين في المملكة العربية السعودية، وأن عملية التحول الرقمي في صناعة التأمين في مراحلها الأولى وتحتاج إلى جهود مكثفة من قبل الشركات لتحسين جودة الخدمات الإلكترونية المقدمة وتلبية رغبات العملاء، ومن أهم نتائج الدراسة أن عملية التحول الرقمي في قطاع التأمين في المملكة العربية السعودية لا زالت تحتاج إلى تطوير وشركات التأمين العاملة في المملكة تحتاج إلى المزيد من الاستثمار في تكنولوجيا المعلومات والبنية التحتية القوية لتقديم الخدمات الإلكترونية بجودة وكفاءة ترضي العملاء.

وتناولت دراسة (Abdelraheem, ١,٢٠٢١) بعنوان: " Dynamic Cyber Security Risk Management using Machine Learning (Intelligence Security Operation Center)". تلك مع إدارة مخاطر الأمن السيبراني التي تتضمن تحديد المخاطر السيبرانية التي تتعرض لها المنظمة ومدى امكانية تطبيق الإجراءات الإدارية والحلول الشاملة للتأكد من أن المنظمة محمية من المخاطر بشكل كافٍ، ويجب أن يكون اختيار إدارة مخاطر الأمن السيبراني المناسبة للتعامل. الهجمات السيبرانية المتغيرة والمستمرة قادراً على تخفيف تأثير تلك المخاطر إلى مستويات مقبولة دون التضحية بأهداف الأمن الرئيسية، وتقوم المنهجيات الحالية بتقييم تأثيرات مخاطر الأمن السيبراني بناءً على نهج إدارة المخاطر التقليدي، حيث تكون البيانات التي تتم مراقبتها ضخمة ومعقدة، مما يزيد من عدد التغيرات الأمنية غير المعروفة والأخطاء المحتملة، مما يؤدي إلى توسيع قنوات الهجوم والتي تحتاج إلى اتخاذ العديد من التدابير الإدارية المخاطر السيبرانية بشكل ديناميكي، وقامت الدراسة باقتراح نموذج يعمل على زيادة كفاءة وموثوقية إدارة مخاطر الأمن السيبراني ولديه القدرة على التعامل . مع البيئة المتغيرة في نظام المعلومات.

وأشارت دراسة (إسماعيل، ٢٠٢١م) بعنوان "التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة - دراسة في القانون القطري والمقارن" إلى أن الشركات التجارية تواجه اليوم تحديات كبيرة في الحفاظ على سياسة الخصوصية، وحماية البيانات، وأمن المعلومات، وإدراكاً لهذه التهديدات تدخلت شركات التأمين، وقدمت منتجاً جديداً نسبياً، وهو التأمين السيبراني، أو ما يطلق عليه التأمين الإلكتروني، ويمثل هذا التأمين استجابة لمطالب الشركات بالدفاع عنها والتخفيف من الأضرار الناتجة عن الهجمات الإلكترونية لإحداث خرق البيانات وانتهاك الخصوصية، وهدف البحث إلى دراسة المشكلات القانونية للتأمين الإلكتروني ضد المخاطر السيبرانية، في الوقت الذي تزداد فيه الهجمات الإلكترونية، ويزيد بالمقابل الطلب على التأمين الإلكتروني في ظل الظروف الاستثنائية لجائحة كورونا (كوفيد ١٩)، وقد توصلت الدراسة إلى عدد من النتائج أهمها أن الهجمات الإلكترونية تشكل تهديداً كبيراً على الدول والأفراد والشركات التجارية. مما يتطلب تضافر الجهود من كل الأطراف لمواجهة تلك الهجمات بكافة الطرق والوسائل العلمية الحديثة.

ووضحت دراسة (Metwally, ٢٠٢٢) بعنوان "Internal Auditors' Role in Confronting Cyber and Fraud Risks Related to Outsourcing Insurance: an Exploratory Study" الكيفية التي أثار بها ظهور جائحة فيروس كورونا (Covid-١٩) العديد من المخاوف في نظم الرقابة الداخلية الشركات التأمين ومواجهة مخاطر الاحتيال، حيث أدى ظهور Covid-١٩ تحولاً هائلاً نحو عمليات التحول الرقمي في معظم الأنشطة الخدمية للشركة، ووجدت شركات التأمين نفسها تعتمد على الاستعانة بمصادر خارجية كوسيلة للتعامل مع تغييرات ومتطلبات السوق، حيث زاد هذا التغيير من مخاطر الهجمات والتهديدات السيبرانية الإلكترونية، ويمثل ذلك خطراً كبيراً على شركات التأمين من أي خطر آخر لأنه لن يعرض شركات التأمين للتقاضي بشأن انتهاكات البيانات فحسب، بل سيؤدي أيضاً إلى إلحاق ضرر جسيم بسمعة شركة التأمين عند حدوث هجوم. علاوة على ذلك بسبب عمليات التحول الرقمي فإنه من الصعب إدارة مخاطر الاحتيال، حيث إن الضوابط الداخلية التقليدية قد تؤدي إلى تأخير دفع مطالبات (تعويضات التأمين مما قد يثير مخاوف بشأن سمعة شركة التأمين، ووضحت الدراسة كيفية مواجهة شركات التأمين للمخاطر السيبرانية الناتجة عن استخدام شبكة الإنترنت، وقدمت الدراسة بعض الحلول التي من شأنها أن تساعد المراجعين الداخليين في التغلب على المخاطر والتهديدات السيبرانية الناتجة عن استخدام شبكة الانترنت في ممارسة الأنشطة الخدمية لشركات التأمين.

وجاءت دراسة (المنصور، ٢٠٢٢م) بعنوان "إدارة المخاطر وإستراتيجية التأمين في ظل تكنولوجيا المعلومات" لتحليل إدارة المخاطر وإستراتيجية التأمين غير التجاري في ظل تكنولوجيا المعلومات، حيث تمثل مخاطر تكنولوجيا المعلومات أحد هذه المخاطر، والتأمين أحد الوسائل لمواجهة الكثير من المخاطر والتهديدات السيبرانية الناتجة عن التكنولوجيا المعلوماتية، ويتم مواجهة تلك المخاطر بإستراتيجية التأمين من خلال الإدارة الفعالة للمخاطر، وتبني فلسفة علمية اجتماعية في إدارة المخاطر، ومن أهم نتائج الدراسة وضع خطوط عامة لإستراتيجية تأمين فعالة في إطار مفهوم وفلسفة متجددة لإدارة المخاطر، والانتقال من مفهوم إدارة المخاطر التقليدية إلى إدارة المخاطر الواقعية.

وأكدت دراسة (Wang, ٢٠٢٣) بعنوان "Research on Digital Transformation in the Insurance Industry" على أن التحول الرقمي أصبح خياراً إستراتيجياً للشركات بما في ذلك صناعة التأمين، وقد شهدت صناعة التأمين تحولاً ملحوظاً في استخدام تقنيات المعلومات وتبنيها تقنيات حديثة مثل تحليل البيانات الضخمة والذكاء الاصطناعي وانترنت

الأشياء لتحسين العمليات التشغيلية، إذ أن التحول الرقمي بعد اتجاهها حتمياً لا مفر منه، ومن الأسباب التي دعت إلى اللجوء إلى عمليات التحول الرقمي في صناعة التأمين وجود تحديات واجهت قطاع التأمين خلال انتشار كوفيد ١٩ ، مما نتج عن التحول الرقمي إلى الحصول على منتجات أكثر تخصصاً وقابلة للتسويق، وأيضاً ازدياد الطلب على منتجات تأمينية مبتكرة لسد احتياجات العملاء المتغيرة، والتحول نحو الإدارة الرقمية عبر التسويق وخدمة العملاء، كذلك تطوير منتجات تأمين أكثر تخصيصاً وتعزيز عمليات صنع القرار والعمليات المستندة إلى البيانات، وتحقيق قدرة تنافسية أفضل في سوق التأمين من خلال الأعمال المدعومة بالتكنولوجيا. ومن أهم نتائج الدراسة تأكيداً على أهمية التحول الرقمي في صناعة التأمين، وكذلك أهمية الحاجة إلى التكنولوجيا والأعمال عبر الاتصال بالإنترنت مما يساهم في استدامة وازدهار شركات التأمين على المدى الطويل، كما تعتبر الدراسة مصدراً قيماً لصانعي السياسات والجهات التنظيمية لوضع إرشادات متعلقة بتطبيق التحول الرقمي في قطاع التأمين.

وناقشت دراسة (جعفر، ٢٠٢٤م) بعنوان " أثر التحول الرقمي على إدارة مخاطر التأمين باستخدام تحليل السيناريوهات واختبار الإجهاد " تأثير التحول الرقمي على إدارة المخاطر في قطاع التأمين، وركزت الدراسة على كيفية استخدام تحليل السيناريوهات واختبار الإجهاد لتحسين فعالية العمليات التأمينية، وهدفت إلى استكشاف التحديات والفرص التي يواجهها قطاع التأمين في ظل التحول الرقمي، وكيف يمكن لهذه التقنيات أن تعزز من قدرة الشركات على إدارة المخاطر بشكل أكثر كفاءة.

وهدفت دراسة (الكرعاوي، ٢٠٢٤م) بعنوان " دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين " إلى دراسة العلاقة بين التدقيق الداخلي وإدارة مخاطر الأمن السيبراني في الوحدات الاقتصادية فضلاً عن معرفة قدرة التدقيق الداخلي من خلال إدارة مخاطر الأمن السيبراني في خفض تكلفة التأمين من خلال الحد من قوة هذه المخاطر على الوحدات الاقتصادية ، ومن أهم نتائج الدراسة أن هناك تأثير ذو دلالة إحصائية للتدقيق الداخلي في إدارة مخاطر الأمن السيبراني وانعكاسه على كلف التأمين.

المنطلقات النظرية للدراسة:

(١) مفهوم المخاطر السيبرانية:

تعرف المخاطر السيبرانية بأنها جميع المخاطر التي تتعلق بشبكة الانترنت، والسيبرانية جاءت من كلمة (Cyber) باللغة الإنجليزية، وهي مشتقة من كلمة (Cybernetics) وتعني (علم التحكم الآلي) الذي صاغه عالم الرياضيات الأمريكي Norbert Wiener، وفي دراسة (بانافا، ٢٠١٩م) تعني المخاطر السيبرانية " بأنها ترابط البنى التحتية لشبكات تكنولوجيا المعلومات وتضم أدوات أو وسائل التكنولوجيا مثل الانترنت"، وعرفها الربيع، (٢٠١٨ م) بأنها "تعني صفة لأي شيء مرتبط بثقافة الحاسبات الآلية أو تقنية المعلومات أو الواقع الافتراضي.

(٢) مفهوم الأمن السيبراني:

يلعب الأمن السيبراني دوراً حاسماً في إدارة العديد من المخاطر الالكترونية لجميع المؤسسات الاقتصادية ومنها شركات التأمين، خاصة في ظل التطور التكنولوجي المتسارع، وزيادة الاعتماد على الأنظمة الرقمية، وتنوع التهديدات والمخاطر السيبرانية المرتبطة بالبيانات وتكنولوجيا المعلومات في الأعمال التجارية، وتناولت العديد من الدراسات السابقة المرجعية العديد من تعريفات للأمن السيبراني، فعرفه الاتحاد الدولي للاتصالات (ITU) بأنه "مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية، والمبادئ ومنهجيات إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات والضمانات والتقنيات التكنولوجية التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصفة عامة".

(٣) إدارة المخاطر السيبرانية:

إدارة المخاطر السيبرانية هي عملية منهجية تهدف إلى تحديد وتقييم والتحكم في المخاطر المرتبطة بالتهديدات السيبرانية التي قد تؤثر على المعلومات والأنظمة الرقمية للمؤسسة. تشمل هذه العملية، تحديد المخاطر من خلال التعرف على التهديدات المحتملة ونقاط الضعف في الأنظمة. وتقييم المخاطر وتحليل المخاطر لتحديد احتمال حدوثها وتأثيرها المحتمل على الأعمال. بالإضافة إلى استراتيجيات التحكم وتطوير استراتيجيات للتقليل من المخاطر، مثل تنفيذ التدابير الأمنية والتدريب. وأخيراً المراقبة والتقييم المستمر ومتابعة فعالية استراتيجيات إدارة المخاطر وتحديثها بناءً على التغيرات في البيئة السيبرانية. والتخطيط للطوارئ ووضع خطط للاستجابة السريعة في حالة حدوث خرق أمني أو هجوم سيبراني. حيث تهدف إدارة المخاطر السيبرانية إلى حماية الأصول الرقمية وتقليل فرص حدوث الحوادث التي قد تؤثر على سمعة المؤسسة وأمن المعلومات.

المنهجية وطرق البحث:

يعتمد البحث على عدة مناهج بحثية لتحقيق التكامل بين الجانب العلمي والعملية. حيث تم الاعتماد على المنهج الاستقرائي، من خلال استعراض واستقصاء البحوث والدراسات المتعلقة بمفهوم جودة الأرباح والمقاييس المستخدمة في قياسها لبناء النموذج المقترح. كما تم الاعتماد على منهج تحليل المحتوى، من خلال تحليل الأفكار والعلاقات والمداخل والجوانب العملية والعلمية التي تتضمنها الدراسات المستقاة لتحقيق أهداف البحث.

أدوات الدراسة:

سوف يتم الاعتماد على استبيان كأداة رئيسية لجمع البيانات حول إدارة مخاطر الأمن السيبراني في شركات التأمين. ويتضمن الاستبيان عدة محاور أهمها مستوى الوعي بمخاطر الأمن السيبراني، أهمية الأمن السيبراني، استراتيجيات إدارة المخاطر، كفاءة إدارة المخاطر، التحديات التي تواجه إدارة المخاطر السيبرانية. وتشمل الفئة المستهدفة من الاستبيان كل من موظفو شركات التأمين، والعاملون في مختلف الأقسام، مثل الأمن السيبراني، تكنولوجيا المعلومات، وإدارة المخاطر، والأفراد المسؤولون عن إدارة استراتيجيات الأمن السيبراني داخل الشركات. سيتم تحليل البيانات من خلال استخدام تقنيات التحليل الإحصائي لاستخراج الأنماط والاتجاهات من البيانات. وسيتم استخدام مقاييس مثل المتوسطات والانحرافات المعيارية. ثم يتم تفسير النتائج بناءً على الأهداف البحثية، مع تسليط الضوء على العلاقة بين مستوى الوعي بمخاطر الأمن السيبراني وفعالية استراتيجيات الإدارة.

حدود الدراسة:

- ١- الحدود الموضوعية: يركز البحث على إدارة مخاطر الأمن السيبراني في شركات التأمين، ولا يتناول مجالات أخرى من الأمن السيبراني خارج هذا القطاع.
- ٢- الحدود المكانية: سيتم تطبيق الدراسة على أفرع وكاتب مؤسسة التأمين بالمملكة العربية السعودية.
- ٣- الحدود الزمنية: تشمل الدراسة البيانات المستمدة من الاستبيانات التي سيتم جمعها خلال العام الحالي، مع الإشارة إلى الممارسات الحالية والتحديات في السنوات الأخيرة. خلال الفترة الزمنية التي تشمل النصف الثاني من العام الجامعي ٢٠٢٥م.
- ٤- الحدود البشرية: تستهدف الدراسة موظفي شركات التأمين، بما في ذلك العاملين في الأقسام المتعلقة بالأمن السيبراني وتكنولوجيا المعلومات وإدارة المخاطر، بالإضافة إلى المدراء التنفيذيين والمختصين في هذا المجال.

- (١) إسماعيل، محمد، (٢٠٢١)، التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن" المجلة الدولية للقانون، جامعة قطر.
- (٢) زيد، أيمن، العمودي، (٢٠١٥)، إدارة المخاطر في شركات التأمين دراسة قياسية بالتطبيق على الشركات الجزائرية للتأمين، مجلة رؤى اقتصادية والتجارية وعلوم التسيير، العدد ٩.
- (٣) الكرعوي، زهراء، (٢٠٢٤)، دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين، مجلة الغري للعلوم الاقتصادية والإدارية، كلية الغدادة، مجلد ٢٠.
- (٤) مروة، القصاص، (٢٠١٧)، دور نظم المعلومات الإلكترونية في إدارة مخاطر الصناعة التأمينية دراسة حالة عينة من شركات التأمين الجزائرية"، قسم العلوم الاقتصادية والقانونية، العدد ١٨.
- 5) Smali, N., Radu, C. and Khalili, A. (2022), "Board effectiveness and cybersecurity disclosure", Journal of Management and Governance, pp.1-23.
- 6) Kamiya, S., Kang, J.K., Kim, J., Milionis, A. and Stulz, R.M. (2021), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", Journal of Financial Economics, Vol. 139No.3, pp. 719-749.
- 7) Shackelford, Scott J, (2012), "Should your firm invest in cyber risk insurance?" Business Horizon Journal Vol. 55 No. 4, August, pp. 349-356.
- 8) Young, D., Lopez, J., Jr, Rice, M., Ramsey, B. and McTasney, R. (2016), "A framework for incorporating insurance in critical infrastructure cyber risk strategies", International Journal of Critical Infrastructure Protection, Vol. 14, pp. 43-57.
- 9) Talesh, S.A. (2018), "Data breach, privacy, and cyber insurance: how insurance companies act as 'compliance managers' for businesses", Law and Social Inquiry, Vol. 43 No. 2, pp. 417-440.
- 10) Abdelraheem, M, (2021), Dynamic Cyber Security Risk Management (Intelligence Security Operation Center) using Machine Learning , Master of Science in Data Science, Princess Sumaya University for Technology, King Abdullah I School of Graduate Studies and Scientific Research, pp.1-102.
- 11) Wang, W, (2023)," Research on Digital Transformation in the Insurance Industry" International Conference on Management Research and Economic Development, pp.100-106.