

### عنوان البحث

إدارة مخاطر الأمن السيبراني في شركات التأمين

بالتطبيق على

قطاع التأمين بالمملكة العربية السعودية

إعداد الطالب/ عبدالله أحمد الجنيد

العام الدراسي:

2025م

## حقوق الطباعة

حقوق الطباعة تمتلكها جامعة ميدأوشن. حيث إن جميع المواد والمحتويات الواردة في هذا البحث هي ملك

للجامعة، ولا يجوز استخدامها أو إعادة نشرها أو توزيعها بدون إذن مسبق من جامعة ميدأوشن.

الباحث

## المستخلص

تتناول هذه الدراسة أهمية إدارة مخاطر الأمن السيبراني في قطاع التأمين بالمملكة العربية السعودية، حيث تزايدت الهجمات السيبرانية وانتهاكات البيانات بشكل ملحوظ في السنوات الأخيرة. كما تهدف الدراسة أيضاً إلى تقييم فعالية استراتيجيات إدارة المخاطر السيبرانية وتحديد التحديات التي تواجهها الشركات في هذا المجال. تم استخدام استبيان شامل لجمع البيانات من العاملين في القطاع التأميني، حيث تم تحليل استجابات المشاركين لتحديد مستوى الفعالية والالتزام في تطبيق تكنولوجيا المعلومات وإدارة المخاطر. أظهرت النتائج وجود مستوى إيجابي عام في تقييم إدارة استثمارات تكنولوجيا المعلومات، مع متوسط بلغ 4.03. كما أظهرت النتائج أهمية تدريب العاملين، حيث حصلت الفقرة المتعلقة بتدريبهم على متوسط 3.54، مما يشير إلى التزام القطاع بتعزيز الوعي الأمني. وقد كشفت الدراسة أيضاً عن وجود فروق معنوية في الاستجابات تعزى لمتغير الفئة الوظيفية، حيث كان للعاملين في إدارات الأمن السيبراني ونظم المعلومات توجه أكبر نحو تطبيق إدارة المخاطر. ومع ذلك، لم تؤثر متغيرات المؤهل العلمي وعدد سنوات الخبرة على استجابات المشاركين. وتوصي الدراسة بتعزيز برامج التدريب، وتحسين الهيكل التنظيمي لدعم إدارة المخاطر، وتحديث الأنظمة بشكل دوري. كما تشير النتائج إلى ضرورة تطوير استراتيجيات فعالة لتحسين الأداء وتعزيز تجربة العملاء في القطاع التأميني. يساهم هذا البحث في تقديم رؤية قيمة حول كيفية تعزيز الأمن السيبراني في قطاع التأمين، مما يعزز من قدرة المؤسسات على مواجهة التهديدات السيبرانية المتزايدة.

الكلمات المفتاحية: الأمن السيبراني - إدارة المخاطر - قطاع التأمين - تكنولوجيا المعلومات - تقييم المخاطر -

تدريب العاملين - حماية البيانات - المملكة العربية السعودية - التهديدات السيبرانية.

## الشكر والتقدير

أود أن أعبر عن امتناني العميق لكل من أسهم في إنجاز هذه الدراسة. أولاً، أشكر الله سبحانه وتعالى. كما أود أن أوجه الشكر لعائلتي وأصدقائي على دعمهم وتشجيعهم خلال الأوقات الصعبة، حيث كان إيمانهم بقدراتي دافعاً مهماً لي.

كما أعبر عن تقديري لجامعة ميدأوشن لتوفيرها بيئة أكاديمية ملائمة والدعم اللازم، فقد كانت الموارد والتسهيلات المقدمة لها حيوية في إتمام هذا العمل.

وأشكر المشرفين، \_\_\_\_\_، على توجيهاتهم القيمة

وملاحظاتهم التي ساعدت في تحسين جودة البحث.

كما أقدر المساهمة القيمة للدكاترة المحكمين للاستبيان ولعينة البحث، حيث كان تبادل المعلومات والخبرات بينهم له تأثير إيجابي على عمق الدراسة.

أخيراً، أشكر كل من دعموني، فهذه الدراسة ثمرة جهود جماعية، وأنا ممتن لكل من ساهم فيها.

الباحث

## فهرس المحتويات

|    |                                                               |
|----|---------------------------------------------------------------|
| 2  | ..... حقوق الطباعة                                            |
| 3  | ..... المستخلص                                                |
| 4  | ..... الشكر والتقدير                                          |
| 5  | ..... فهرس المحتويات                                          |
| 7  | ..... قائمة الجداول                                           |
| 8  | ..... مصطلحات البحث                                           |
| 11 | ..... الفصل الأول: المدخل العام للبحث                         |
| 12 | ..... مشكلة الدراسة                                           |
| 13 | ..... تساؤلات الدراسة الرئيسي                                 |
| 13 | ..... تساؤلات الدراسة الفرعية                                 |
| 13 | ..... أهمية الدراسة                                           |
| 15 | ..... أهداف الدراسة                                           |
| 15 | ..... فرضيات الدراسة                                          |
| 16 | ..... نموذج الدراسة                                           |
| 16 | ..... خاتمة الفصل                                             |
| 19 | ..... الفصل الثاني: الدراسات السابقة والإطار النظري           |
| 19 | ..... مقدمة                                                   |
| 20 | ..... الدراسات السابقة                                        |
| 27 | ..... الإطار النظري                                           |
| 27 | ..... مقدمة                                                   |
| 28 | ..... 1- المخاطر السيبرانية التي تتعرض لها شركات التأمين      |
| 29 | ..... ٢- أسباب تعرض شركات التأمين للمخاطر السيبرانية          |
| 29 | ..... 3- أنماط التهديدات والهجمات السيبرانية في شركات التأمين |
| 30 | ..... 4- أهمية الأمن السيبراني في شركات التأمين               |
| 32 | ..... 5- دور الأمن السيبراني في إدارة مخاطر شركات التأمين     |
| 32 | ..... 6- منع الهجمات السيبرانية                               |
| 33 | ..... 7- التكنولوجيا والتقنيات                                |
| 33 | ..... 8- الأفراد مستخدمي البيانات                             |
| 34 | ..... 9- الاستجابة والتواصل:                                  |
| 34 | ..... مراحل إدارة المخاطر السيبرانية بشركات التأمين           |
| 37 | ..... المعالجة أو الاستجابة للمخاطر السيبرانية                |

|    |                                                                                  |
|----|----------------------------------------------------------------------------------|
| 37 | متابعة المخاطر السيرانية.....                                                    |
| 37 | مستوى المخاطر السيرانية المقبول.....                                             |
| 38 | مراقبة ومراجعة المخاطر السيرانية.....                                            |
| 40 | الفصل الثالث: منهجية الدراسة .....                                               |
| 40 | مقدمة .....                                                                      |
| 40 | منهج الدراسة.....                                                                |
| 41 | أدوات الدراسة .....                                                              |
| 41 | حدود الدراسة .....                                                               |
| 42 | مجتمع وعينة البحث .....                                                          |
| 42 | خصائص أفراد عينة البحث (المتغيرات الديموغرافية).....                             |
| 43 | أداة البحث .....                                                                 |
| 44 | ثبات أداة الدراسة .....                                                          |
| 44 | إجراءات تطبيق الدراسة.....                                                       |
| 45 | أساليب التحليل الإحصائية .....                                                   |
| 47 | صدق فقرات أداة الدراسة .....                                                     |
| 48 | ثبات الاستبانة (Reliability) .....                                               |
| 50 | نتائج الدراسة ومناقشتها وتفسيرها .....                                           |
| 50 | البعد الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيراني.....                |
| 54 | ثانياً: المحور الثاني (طبيعة ومحددات المخاطر السيرانية بشركات التأمين).....      |
| 58 | ثانياً: المحور الثالث (مدى مساهمة إدارة المخاطر السيرانية في قطاع التأمين) ..... |
| 62 | معنوية الفروق في اتجاهات المستجيبين تعزى للمتغيرات الديموغرافية" .....           |
| 62 | الفئة الوظيفية.....                                                              |
| 63 | المؤهل العلمي.....                                                               |
| 64 | عدد سنوات الخبرة.....                                                            |
| 65 | الخاتمة.....                                                                     |
| 65 | النتائج .....                                                                    |
| 67 | التوصيات .....                                                                   |

## قائمة الجداول

|                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|
| جدول رقم (1): خصائص أفراد عينة البحث                                                                      |
| جدول رقم (2): معامل الثبات ألفا كرونباخ لكل من المحاور الفرعية وإجمالي الاستبيان                          |
| جدول رقم (3): درجات المقياس الخماسي لليكرت                                                                |
| جدول (4): حدود متوسطات استجابات أفراد الدراسة وفقاً لفئات مقياس ليكرت الخماسي                             |
| جدول رقم (5): صدق الاتساق الداخلي لمحاور الدراسة                                                          |
| جدول رقم (6): معامل الثبات ألفا كرونباخ لمحاور الاستبيان                                                  |
| جدول رقم (7): محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني (المحور الأول)                             |
| جدول رقم (8): المتوسط الحسابي والانحراف للمحور الثاني طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     |
| جدول رقم (9): المتوسط الحسابي والانحراف للمحور الثالث مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين |
| جدول رقم (10): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً للفئة الوظيفية                    |
| جدول رقم (11): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً للمستوى التعليمي                  |
| جدول رقم (12): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً لعدد سنوات الخبرة                 |

## قائمة الأشكال

|                                                                                                          |
|----------------------------------------------------------------------------------------------------------|
| شكل رقم (1): المتوسط الحسابي والانحراف للمحور الأول محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني     |
| شكل رقم (2): المتوسط الحسابي والانحراف للمحور الثاني طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     |
| شكل رقم (3): المتوسط الحسابي والانحراف للمحور الثالث مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين |

## مصطلحات البحث

### 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 (الريبعة، ٢٠١٨ م) بأنها "تعني صفة لأي شيء مرتبط بثقافة الحاسبات الآلية أو تقنية المعلومات أو الواقع الافتراضي.

### 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 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".

## 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.

## الفصل الأول

### المدخل العام للبحث

## الفصل الأول: المدخل العام للبحث

### 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، وتمثل هذه المخاطر في إمكانية توافر مجموعة من العوامل بصورة تؤدي إلى نتائج غير مرغوب فيها، هذه العوامل قد تتعلق بالمخاطر المرتبطة بالاكتتاب 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.

#### تساؤلات الدراسة الرئيسي

"ما هو أثر تطبيق إدارة مخاطر الامن السيبراني على شركات التأمين؟"

#### تساؤلات الدراسة الفرعية

- 1- ما هي المخاطر السيبرانية الأكثر شيوعًا التي تواجه شركات التأمين في المملكة العربية السعودية؟
- 2- كيف يتم تقييم الوضع الحالي لإدارة مخاطر الأمن السيبراني في قطاع التأمين؟
- 3- ما هي الاستراتيجيات والممارسات الحالية التي تتبعها شركات التأمين في إدارة المخاطر السيبرانية؟
- 4- كيف يمكن تصميم نموذج متكامل لإدارة مخاطر الأمن السيبراني يتناسب مع احتياجات شركات التأمين في المملكة؟

#### 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 نموذجًا مقترحًا 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 رؤى 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.

## فرضيات الدراسة

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

- فرضية الدراسة الأول: 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.

#### نموذج الدراسة

#### المتغيرات

- محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني
- طبيعة ومحددات المخاطر السيبرانية بشركات التأمين
- مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين

#### خاتمة الفصل

عرض الفصل المحاور الرئيسية التي ستعتمد عليها الدراسة، حيث تضمن مشكلة الدراسة والتي ركزت على فهم التحديات التي تواجه قطاع التأمين في المملكة العربية السعودية، حيث أصبحت الهجمات السيبرانية وانتهاكات البيانات تهديدات متزايدة تستنزف موارد المؤسسات وتؤثر سلباً على سمعتها. يعكس النمو المتسارع في أسواق الأمن السيبراني الحاجة الملحة لحماية البيانات والبنية التحتية الرقمية، مما يجعل الأمن السيبراني جزءاً لا يتجزأ من استراتيجيات الحكومات والشركات الكبرى. أما أهمية الدراسة، فتتجلى في دورها البارز في تعزيز الفهم الأكاديمي والعملي للأمن السيبراني، حيث تساهم في إثراء الأدبيات الأكاديمية وتقديم نموذج مقترح لإدارة المخاطر، مما يعزز من التعاون

بين مجالات الأمن السيبراني وإدارة المخاطر. على المستوى العملي، يوفر النموذج استراتيجيات فعالة لتحسين مستوى الأمان وتعزيز ثقة العملاء، مما يساهم في تقليل المخاطر القانونية والمالية. وقد تضمنت أهداف الدراسة تحديد دور الأمن السيبراني في إدارة مخاطر شركات التأمين، مع التركيز على التعرف على المفاهيم المرتبطة بالمخاطر، وتحليل التحديات، ودراسة الوضع الحالي، وتصميم نموذج متكامل لإدارة المخاطر. كما استندت الدراسة إلى فرضيات تشير إلى وجود علاقة بين إجراءات الأمن السيبراني ومستوى إدارة المخاطر، مما يعزز من أهمية البحث في فهم كيفية تأثير هذه الإجراءات على فعالية إدارة المخاطر في الشركات. وفي الختام، يعكس هذا الفصل أهمية البحث في مواجهة تحديات الأمن السيبراني، ويؤكد على ضرورة تطوير استراتيجيات فعالة تساهم في حماية قطاع التأمين وتوفير بيئة آمنة للمعلومات والبيانات.

## الفصل الثاني

### الدراسات السابقة والإطار النظري

## الفصل الثاني: الدراسات السابقة والإطار النظري

### مقدمة

يعتبر الفصل الثاني والمتضمن الإطار النظري حجر الزاوية لأي دراسة علمية، حيث يحدد الأسس المفاهيمية والنظرية التي يستند إليها البحث. في هذا الفصل، سيتم تناول المفاهيم الأساسية المتعلقة بإدارة مخاطر الأمن السيبراني، خاصة في سياق قطاع التأمين، حيث تمثل هذه المفاهيم الإطار الذي يمكن من خلاله فهم التحديات والفرص المرتبطة بالأمن السيبراني. وتزايد أهمية الأمن السيبراني في عصر تتسارع فيه التطورات التكنولوجية وتزداد فيه التهديدات الإلكترونية. لذا، فإن فهم المخاطر السيبرانية وأساليب إدارتها يصبح أمرًا بالغ الأهمية. سيستعرض هذا الفصل المفاهيم الأساسية المتعلقة بالأمن السيبراني، بما في ذلك تعريفاته، أنواعه، وأهميته في حماية البيانات والبنية التحتية للمؤسسات. كما سيتم استعراض الدراسات السابقة التي تناولت موضوع إدارة مخاطر الأمن السيبراني، مما سيوفر سياقًا لفهم كيفية تطور هذا المجال. ستساعد هذه الدراسات في تسليط الضوء على التحديات التي تواجه الشركات في تنفيذ استراتيجيات فعالة للأمن السيبراني، كما ستساهم في تحديد الفجوات البحثية التي يسعى البحث الحالي إلى معالجتها. من خلال هذا الفصل، سيتم بناء قاعدة معرفية متينة تدعم البحث الحالي، مما يسهل على القراء فهم الروابط بين المفاهيم النظرية والممارسات العملية في إدارة مخاطر الأمن السيبراني. في النهاية، سيسهم هذا الإطار النظري في توضيح أهمية تطوير نموذج متكامل لإدارة المخاطر يتماشى مع احتياجات قطاع التأمين في المملكة العربية السعودية، ويعزز من قدرته على مواجهة التهديدات السيبرانية المتزايدة.

## 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, 2012) 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, 2016) 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.

وهدف 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 دورا حاسما 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 بعيدا 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، ٢٠١٩ م) 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, 2021) 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 قادرا 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 الثغرات 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,2022) بعنوان " Internal Auditors' Role in Confronting Cyber and Fraud " الكيفية التي أثار بها ظهور جائحة فيروس كورونا (Covid-19) العديد من المخاوف في نظم الرقابة الداخلية الشركات التأمين ومواجهة مخاطر الاحتيال، حيث أدى ظهور Covid-19 إلى 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,2023) 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 تحولا ملحوظا في استخدام تقنيات المعلومات وتبنيها تقنيات حديثة مثل تحليل البيانات الضخمة والذكاء الاصطناعي وانترنت الأشياء لتحسين العمليات التشغيلية، اذ أن التحول الرقمي بعد اتجاها حتميا لا مفر منه، ومن الأسباب التي دعت إلى اللجوء إلى عمليات التحول الرقمي في صناعة التأمين وجود تحديات واجهت قطاع التأمين خلال انتشار كوفيد 19 ، 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 تأكيدها 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.

## الإطار النظري

### مقدمة

أصبحت المعلومات في القرن الواحد والعشرين هي عملة العالم الرئيسية، لذا أصبحت الدول والأفراد يتجهون على نحو متزايد نحو تكنولوجيا المعلومات، بما فيها تقنيات الحاسبات والاتصالات، واتجهت جميع المؤسسات للاعتماد في إدارتها على تكنولوجيا المعلومات وشبكات الاتصال، وبالتالي أصبحت الحروب السيبرانية هي الأكثر بروزاً وانتشاراً على الساحة الدولية في الوقت الحالي، وأصبح الفضاء الإلكتروني أهم الأسلحة الاستراتيجية التي تستخدمها الدول في الحروب الحديثة. (لين، ٢٠١٢م) وتشكل المخاطر السيبرانية في بيئتنا الرقمية خطراً كبيراً، وتصنف الحوادث السيبرانية على أنها الخطر الأكبر الذي يواجه الشركات التجارية على مستوى العالم في مقياس 2020 (Allianz) للمخاطر، ولقد نما الوعي بالتهديد السيبراني بسرعة في السنوات الأخيرة مدفوعاً باعتماد الشركات المتزايد على بياناتها وأنظمة تكنولوجيا المعلومات، وعدد من الحوادث البارزة، وتواجه الشركات عدداً متزايداً.

من المخاطر الإلكترونية ذات الهجمات المتطورة التي تستهدف بشكل خاص الشركات الكبيرة والمتوسطة، وزيادة في حوادث برامج الفدية واختراق البريد الإلكتروني للأعمال التجارية ومطالب ابتزاز ضخمة. (إسماعيل، ٢٠٢١م) والجدير بالذكر أن قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة ٧٠% وفق تقديرات البنك الدولي وقد تصل تكلفة الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو ٣٠٠ إلى ٣٨٠ مليار دولار سنوياً حال اتساع نطاق انتشارها. (صندوق النقد العربي، ٢٠١٩م) وتوضح تقديرات صندوق النقد الدولي (2024 Global Financial Stability Report) أن عدد حوادث الأمن السيبراني في القطاع المالي في نهاية عام ٢٠٢٣م تعدى ٢٠ ألف هجوم سيبراني، وبلغت الخسائر المباشرة الناجمة عن حوادث الأمن السيبراني أكثر من ١٢ مليار دولار، كما أوضح أن القطاع المالي تعرض إلى أكثر من ٢٠% من عدد الهجمات السيبرانية، وأن الجرائم الإلكترونية ستكلف العالم حوالي

٢٣ ترليون دولار أمريكي في عام ٢٠٢٧م، بزيادة قدرها ١٧٥% عن عام ٢٠٢٢م ، كما أن هناك زيادة للتهديدات السيبرانية المشفرة بنسبة ٩٢% خلال عام ٢٠٢٤م، وزيادة البرامج الضارة بنسبة ٣٠% عن عام ٢٠٢٣م.

ومن المتوقع أن يصل حجم سوق الأمن المعلوماتي عالمياً إلى ٢٥٠ مليار دولار بحلول عام ٢٠٢٦م، مع معدل نمو سنوي مركب يتراوح من ١٢ - ١٥% خلال السنوات القادمة نتيجة لعدة عوامل أهمها: تزايد الهجمات السيبرانية التحول الرقمي السريع زيادة الاعتماد على التقنيات السحابية، تعزيز الامتثال للقوانين والتشريعات)، وعلى مستوى منطقة الشرق الأوسط وشمال إفريقيا فمن المتوقع أن يصل حجم الإنفاق على الأمن السيبراني إلى حوالي خمسة مليارات دولار بحلول عام ٢٠٢٦م، مع معدل نمو سنوي مركب يتراوح من ٩% - ١٠% (المؤتمر العربي لأمن المعلومات، ٢٠٢٥م)

#### 1- المخاطر السيبرانية التي تتعرض لها شركات التأمين

تتعرض شركات التأمين للعديد من المخاطر خاصة المخاطر التشغيلية، وهي مخاطر الخسارة المترتبة عن المشاكل الناتجة عن التعاملات مع الأطراف الأخرى أو عدم كفاءة العمليات الداخلية أو فشلها، والتي تشمل الأخطاء التي يرتكبها الموظفون وفشل الأنظمة والحرائق والفيضانات أو غيرها من الخسائر المادية، كذلك الاحتيال أو أي نشاط إجرامي آخر، ووفقاً للجنة بازل (II) فقد عرفت المخاطر التشغيلية بأنها "مخاطر الخسائر الناتجة عن عدم كفاية أو فشل العمليات الداخلية، أو الأفراد، أو الأنظمة، أو عن أحداث خارجية" (سعد، وآخرون، ٢٠٢١م)، ومن خلال تعريف لجنة بازل للمخاطر التشغيلية نجد أن المخاطر السيبرانية تندرج تحت هذا النوع من المخاطر، وتعد أكثرها تهديداً لشركات التأمين.

## ٢- أسباب تعرض شركات التأمين للمخاطر السيبرانية

تعتبر شركات التأمين هدفاً طبيعياً للهجمات الإلكترونية لأنها تمتلك كميات كبيرة من بيانات حملة وثائق التأمين السرية، حيث إن منتجات التأمين والسياسات والأسعار جميعها مدعومة بالبيانات والمعلومات، وهذا يجعلها ذات قيمة كبيرة، وعلى عكس القطاعات المالية الأخرى كالبنوك وغيرها التي تحتوي على بيانات مالية حساسة فقط فإن شركات التأمين تجمع نوعين من المعلومات الحساسة لعملائها منه ما هو مالي ومنه ما هو شخصي، كما أن وباء كورونا (Corvid-19) أي إلى تسريع عمليات التحول الرقمي في كافة القطاعات بالدولة ومنها شركات التأمين، ومن ثم زادت المؤسسات المالية من استخدامها لتكنولوجيا المعلومات، حيث أنها تعتمد حالياً بشكل أكبر على الحلول الرقمية لأداء عملياتها اليومية وتقديم خدماتها للعملاء، وبالرغم من المزايا والفوائد التي تعود على شركات التأمين من عمليات التحول الرقمي إلا أن الاعتماد المتزايد عليها ترتب عليه زيادة مخاطر الهجمات الإلكترونية. (Jon & Leonardo, 2021)

## 3- أنماط التهديدات والهجمات السيبرانية في شركات التأمين

قد تنشأ المخاطر السيبرانية من عدد من المصادر، وغالباً ما تكون غير متوقعة، وقد تتنوع التأثيرات وقد تؤثر على الأعمال التجارية بعدة طرق مختلفة، وقد تكون الهجمات على البنية التحتية الحيوية، ويكون لها عواقب بعيدة المدى، وقد ترجع المخاطر والتأثيرات إلى خطأ بشري أو خطأ في النظام، ولكن أيضاً إلى الجريمة الإلكترونية التي غالباً ما تكون مدفوعة بدوافع إجرامية تقليدية، مثل السرقة أو السطو أو التخريب، وبالتالي قد يكون مجرمو الإنترنت داخليين أو خارجيين للمؤسسة، ودوافعهم متنوعة ومتطورة منتدى CRO، ٢٠١٤م)، ومع تزايد الخسائر المحتملة نتيجة استخدام تكنولوجيا المعلومات والبيانات، فمن المتوقع أن تتوقف الشركات عن التعامل مع الهجمات السيبرانية باعتبارها مصدر إزعاج فقط بل يتم التعامل مع مثل هذه الهجمات باعتبارها التهديد الخطير الذي يتوقف عليه بقاء تلك الشركات في السوق (Shackelford, S.J. 2012).

وتتعدد أنماط التهديدات والهجمات السيبرانية التي تتعرض لها شركات التأمين، حيث بلغت نسبة عمليات التصيد الاحتيالي للمعلومات ٨٠% من الهجمات الإلكترونية، كما تبين أن ٧١% من الهجمات يركز على سرقة تفاصيل الدخول (Ukwanda et al,2022) ويمكن تلخيص التهديدات السيبرانية في نوعين أساسيين وهما كالآتي:

- التهديدات الداخلية: وهي المخاطر الناتجة عن الموارد البشرية داخل شركة التأمين، وتنشأ من خلال العاملين في المؤسسة الذين يضطعون على أنشطتها ويعملون كجزء من أنظمة معلوماتها، وأيضاً تسريب المعلومات عن طريق مستخدمو النظام، والمخاطر الناتجة عن التكاليف الباهظة للاستثمار في البنية التحتية التكنولوجية وإعادة هندسة العمليات الداخلية، ومخاطر الكفاءة التشغيلية والإنتاجية. (جعفر، ٢٠٢٤م)

- التهديدات الخارجية: وهي الأكثر خطورة لصعوبة معرفة المخترق وأهدافه من وراء الاختراق ومدى اختراق النظام، ومنها تهديدات البرمجيات وتشمل: حذف البرنامج، أو سرقة، أو تشويهه بسبب تعطيل الأجهزة أو إصابتها بالفيروسات، وتهديدات الأجهزة وتشمل: سرقة الأجهزة أو العبث فيها أو تدميرها، وتهديدات المعلومات وتشمل: حذف المعلومات أو التشويه الناتج عن مشاكل الأجهزة والبرامج والتجسس والابتزاز، واتلاف، وتخريب البيانات، واعتراضها. (بوقرص، ٢٠٢٢م).

#### 4- أهمية الأمن السيبراني في شركات التأمين

ترجع أهمية الأمن السيبراني إلى العديد من الأسباب أهمها: (جعفر، ٢٠٢٤م)

- تطور تهديدات الأمن السيبراني: تتطور التهديدات الإلكترونية باستمرار، ويجب أن تتكيف شركات التأمين مع هذه التغييرات لحماية أنفسها وعملائها، حيث أصبح المتسللون أكثر تطوراً في تكتيكاتهم

ويستهدفون جميع الكيانات الاقتصادية بما في ذلك شركات التأمين، لذلك يجب أن تكون شركات التأمين

على دراية بأحدث المخاطر والتهديدات السيبرانية، وأن تتخذ تدابير استباقية لحماية بياناتها.

- فقدان البيانات السرية التي تتعلق بالعملاء: أكدت تقارير صادرة عن البنك الدولي على أن نسبة العملاء الذين عانوا من الهجمات السيبرانية خلال عام ٢٠٢٠ م على المستوى العالمي نحو ٧٢% بزيادة قدرها حوالي 1% مقارنة بعام ٢٠١٩ م ، وتتعامل شركات التأمين مع قدر كبير من البيانات الحساسة مثل المعلومات الشخصية والسجلات المالية والسجلات الطبية للعملاء، وهذه البيانات ذات قيمة عالية لمجرمي الانترنت الذين يمكنهم استخدامها لسرقة الهوية والاحتيال وغيرها من الأنشطة غير القانونية، لذلك يجب أن تضمن شركات التأمين حماية هذه البيانات من خلال تنفيذ تدابير أمنية قوية. (قطيعة، ٢٠٢٣م)

- تعطيل الأعمال بشركة التأمين: لا تنطوي جميع الحوادث السيبرانية على انتهاكات للبيانات فقط، بل تعطيل العمليات التجارية التي تتم من خلال رسائل البريد الإلكتروني ورسائل البريد الصوتي وغيرها من الطرق المستخدمة في تسهيل تقديم الخدمات التأمينية للعملاء.

- الإضرار بسمعة شركة التأمين حيث تعتمد شركات التأمين على سمعتها لجذب العملاء والاحتفاظ بهم، وقد يؤدي خرق الأمن السيبراني إلى إتلاف سمعة شركة التأمين مما يؤدي إلى فقدان العملاء والإيرادات.

- الاحتيال على التأمين يمثل تهديداً حقيقياً إن الاحتيال في التأمين يمثل مشكلة متزايدة، ويستخدم مجرمو الإنترنت التكنولوجيا لارتكاب الاحتيال في التأمين، لذلك يجب على شركات التأمين تنفيذ تدابير لمنع واكتشاف الاحتيال في التأمين، مثل استخدام تحليلات البيانات وخوارزميات التعلم الآلي لتحديد المطالبات الاحتيالية.

##### 5- دور الأمن السيبراني في إدارة مخاطر شركات التأمين

تلعب شركات التأمين دوراً محورياً في تقديم الخدمات التأمينية للأفراد والشركات ضد المخاطر المختلفة، ومع التحول الرقمي المتسارع تواجه شركات التأمين معضلة كبيرة بسبب تزايد مخاطر الأمن الإلكتروني وأصبحت شركات التأمين نفسها كما هي باقي المؤسسات الاقتصادية أكثر عرضة للمخاطر السيبرانية التي تهدد أمن بياناتها وعملائها، وهنا يأتي دور الأمن السيبراني كأداة أساسية في إدارة هذا المخاطر ويمكن توضيح هذا الدور كما يلي:

(Eling,2016)

- حماية البيانات الحساسة في شركات التأمين: تتعامل شركات التأمين مع كم هائل من البيانات مثل المعلومات الشخصية للعملاء وسجلات المطالبات وسجلات التسويات والعمولات المدفوعة وغيرها من التفاصيل المالية المنوط بالشركة الحفاظ عليها وعدم الافصاح بها للغير بشكل مباشر، ويساعد الأمن السيبراني في حماية تلك البيانات من الاختراقات والوصول غير المصرح لها أو إرسال فيروسات الكترونية تؤدي إلى تلفها أو تعطل النظام ككل بشركة التأمين.

الالتزام بالقوانين واللوائح العالمية: تشديد القوانين واللوائح العالمية على ضرورة حماية البيانات الشخصية من الهجمات والتهديدات السيبرانية، ويقوم الأمن السيبراني بضمان التزام شركات التأمين لهذه القوانين مما يقلل من مخاطر الغرامات المالية وفقدان الثقة من العملاء.

##### 6- منع الهجمات السيبرانية

تعتبر شركات التأمين هدفاً جذاباً للقراصنة بسبب قيمة البيانات والمعلومات التي تمتلكها، ويقوم الأمن السيبراني بتوفير طبقات متعددة من الحماية مثل جدران الحماية، وأنظمة كشف التسلل لمنع الهجمات الالكترونية مثل

البرمجيات الخبيثة وهجمات التصيد الاحتيالي. ٥/٤ - إدارة المخاطر السيبرانية يعمل الأمن السيبراني على تحديد وتقييم المخاطر المحتملة عبر تحليل نقاط الضعف في الأنظمة والشبكات، ومن ثم تطوير استراتيجيات استباقية لتقليل هذه المخاطر مثل تحديد البرمجيات بانتظام وإجراء اختبارات الاختراق.

#### 7- التكنولوجيا والتقنيات

حيث تشكل التكنولوجيا والتقنيات دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، ويعمل الأمن السيبراني على حماية الأجهزة بمختلف أشكالها الذكية بالاعتماد على جدران الحماية ومكافحة الفيروسات وغيرها.

#### 8- الأفراد مستخدمي البيانات

يلزم الأمن السيبراني الأفراد من مستخدمي البيانات والأنظمة في شركة التأمين باستخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية وتفادي الروابط الخارجية والمرفقات عبر البريد إلى جانب القيام بعمل نسخ احتياطية للبيانات. إطار عمل الأمن السيبراني في مؤسسات الأعمال: أوضح المعيار (ISO/IEC / 27023:2021) المتعلق بالأمن السيبراني في منظمات الأعمال والصادر عن المنظمة الدولية للمعايير (ISO)، أن إطار عمل الأمن السيبراني يركز على أربع مجالات رئيسية، والتي تعكس أهداف ومدى أهمية وجود نظام للأمن السيبراني بمنظمات الأعمال وعلى رأسها البنوك تم شركات التأمين وهي:

- المنع وذلك من خلال تنفيذ التدابير والضوابط التي تمنع، وتحد من الهجمات الإلكترونية وغيرها من

تهديدات الأمن السيبراني.

- الاكتشاف والحماية وذلك من خلال تطبيق ضوابط إدارة الأمن السيبراني، والمراقبة المستمرة للأحداث

الأمنية، بما يساعد في الاكتشاف المبكر للهجمات الإلكترونية وغيرها من التهديدات السيبرانية وتوفير

الحماية.

#### 9- الاستجابة والتواصل:

وذلك من خلال تنفيذ خطط الطوارئ واتخاذ الإجراءات اللازمة للتصدي للهجمات الإلكترونية بما يضمن

الحفاظ على سرية البيانات وسلامتها وتوافرها، وأيضاً توفير الإبلاغ المناسب عن تلك الهجمات والجهود المبذولة في هذا

المجال. التعافي والتعلم وذلك من خلال تنفيذ إجراءات استعادة أنظمة تكنولوجيا المعلومات والخدمات المتعلقة بها إلى

ما كانت عليه قبل حدوث التهديدات والهجمات الإلكترونية واتخاذ الإجراءات التصحيحية المناسبة لتقليل احتمالات

حدوث مثل هذه الحوادث مجدداً.

#### مراحل إدارة المخاطر السيبرانية بشركات التأمين

يعد الأمن السيبراني جانباً مهماً في صناعة التأمين، ويجب على شركات التأمين اتخاذ تدابير استباقية لحماية

بياناتها وحماية نفسها من التهديدات الإلكترونية من خلال تنفيذ إطار قوي للأمن السيبراني، يمكن لشركات التأمين

التخفيف من خطر الهجمات السيبرانية، والامتثال للوائح وحماية سمعتها، وتشمل مراحل إدارة المخاطر السيبرانية

بشركات التأمين الخطوات التالية:

- تحديد المخاطر السيبرانية: (النجار، ٢٠٢٠م)

تقوم شركة التأمين بتحديد المخاطر السيبرانية المحتملة التي قد تؤثر سلباً على العمليات التشغيلية،

وتحديد بيئة الأعمال والعوامل المساهمة التي تسبب حدوث المخاطر السيبرانية، والأسباب الجذرية لتلك المخاطر،

ووصفها، وفهم الهدف منها، والتهديدات التي تواجه الشركة، ويمكن تحديد المخاطر من مجموعة من المصادر مثل تبادل الأفكار باستخدام أفراد عمليات ذوي خبرة، تطوير سيناريوهات المخاطر المحتملة تطوير برامج تحليل البيانات بيان التحقيقات في الحوادث السيبرانية، وتعدد أدوات تحديد المخاطر السيبرانية في شركات التأمين منها قوائم المراجعة، والدراسات الاستقصائية، وأراء الخبراء في الأمن السيبراني ، وتحليل SWAT ، واستبيانات المخاطر، والسياسات والاستراتيجيات المتبعة لعلاج المخاطر، وطرق ووسائل مراقبة ومتابعة الخطر.

#### - تحليل المخاطر السيبرانية

حيث يتطلب من شركات التأمين دراسة وتحليل أهم المخاطر والتهديدات السيبرانية المحتملة الحدوث، والتي تتعرض لها الشركة، وتحليل أهم الاستراتيجيات المثلى لمواجهتها، (Kamiya, 2019) ، وتتضمن عملية تحليل المخاطر السيبرانية الخطوات التالية: (الخطا، ٢٠٢٠م).

#### - وصف المخاطر

حيث يجب أن يكون هناك بيان موجز لوصف ماهية المخاطر السيبرانية التي تتعرض لها شركة التأمين، وكيف يمكن أن تؤثر على تحقيق الأهداف. - مسببات المخاطر حيث يجب تحديد المسببات المباشرة وغير المباشرة والفهم الجيد لتلك المسببات من أجل تقليل احتمالية حدوث المخاطر بشكل فعال.

#### - الضوابط الوقائية

بعد فهم مسببات المخاطر يتطلب تحديد الضوابط الموجودة بالفعل، تقليل احتمالية حدوث المسببات أو الدوافع وتحديد الضوابط الإضافية والتي تساعد في : التي يمكن وضعها لتقليل الاحتمالية بشكل أكبر.

- نتائج تحقق المخاطر وتعني دراسة الأثر المترتب على تحقق المخاطر السيبرانية، مما يساعد في وضع خطط

للطوارئ في حالة حدوث الخطر مستقبلاً.

- تقييم المخاطر السيبرانية

حيث تحتاج شركة التأمين إلى إجراء تقييم للمخاطر لتحديد نطاق الهجوم السيبراني، وتسمح تقييمات

المخاطر للشركة بفهم أفضل للمناطق ذات أعلى مستوى من المخاطر، وتأثير التهديدات السيبرانية المحتملة، واحتمالية

الهجمات الناجحة، وبالتالي ستكون الشركة مستعدة بشكل أفضل لتخصيص الموارد المناسبة لمجابهة تلك التهديدات،

وما تحتاج إليه لتحقيق أمان كاف للبيانات، والغرض من تقييم المخاطر هو تحديد الآتي: (الخياط ٢٠٢٠م)

- تقييم الضوابط المحتملة ويقصد بها جميع الأدوات والأساليب والعمليات التي تستخدمها الشركة

لتجنب، أو تخفيف أو نقل أو مشاركة المخاطر السيبرانية.

- النظر في برامج التدريب والتوعية المتبعة في الشركة.

- تحديد وتحليل التهديدات الموجهة للمؤسسة من خلال مؤسسات أخرى. - معرفة نقاط الضعف داخل

وخارج المؤسسة.

- تحديد الضرر الذي يحدث في ضوء احتمالية حدوث التهديدات.

- تحديد احتمال وقوع الضرر نتيجة تحقق المخاطر المحتملة.

## المعالجة أو الاستجابة للمخاطر السيبرانية

تتضمن الاستجابة للمخاطر السيبرانية تحديد مجموعة الخيارات لمعالجة المخاطر وتقييمها وإعداد خطط معالجة المخاطر وتنفيذها، وتقوم الإدارة المستولة عن الأمن السيبراني بتحديد الخيارات لمعالجة المخاطر السيبرانية بالخطوات التالية: (Eling,2016)

- معالجة المخاطر أو تقليلها وذلك من خلال تطبيق الضوابط الأمنية اللازمة لتقليل احتمالية الحدوث أو التأثير أو كليهما.
- تجنب المخاطر: أي التخلص من الخطر بتجنب الاستمرار بمصدر الخطر. - مشاركة المخاطر أو تحويلها إلى طرف ثالث لديه الإمكانيات في التعامل مع هذا النوع من المخاطر بشكل أكثر فاعلية.
- تقبل المخاطر وتحملها في حالة ما إذا كان مستوى الخطر مقبول.

## متابعة المخاطر السيبرانية

وهي جزء من خطة التخفيف من المخاطر حيث تقوم على متابعة كل المخاطر السيبرانية من رصد وتتبع المخاطر الجديدة والحالية بشكل مستمر بالإضافة إلى مراجعة عملية إدارة المخاطر الشاملة وتحديثها وفقاً للمواقف المختلفة والمتغيرة، ولتابعة المخاطر السيبرانية يجب أن تعد الإدارة المعنية بالأمن السيبراني بشركة التأمين سجلاً للمخاطر لتوثيق مخرجات عملية إدارة المخاطر السيبرانية على أن يتضمن معلومات عن عملية تحديد المخاطر، ونطاقها والمسئول عن المخاطر، ووصف وتحليل وتقييم المخاطر، وخطة التعامل مع المخاطر). (الرحماوي، ٢٠٢٤م)

## مستوى المخاطر السيبرانية المقبول

يجب تحديد معايير تقبل المخاطر السيبرانية وتوثيقها، وفقاً لمستوى المخاطر، وتكلفة معالجة الخطر مقابل تأثيره من خلال تحديد مدى تأثير الخطر، حيث يتم تصنيف الخطر إلى مخاطر ذات تأثير جسيم مخاطر ذات تأثير

كبير، مخاطر ذات تأثير متوسط، مخاطر ذات تأثير منخفض مخاطر ذات تأثير منخفض جداً، ويجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبل المخاطر.

#### مراقبة ومراجعة المخاطر السيبرانية

إن عملية وصف المخاطر السيبرانية وقياسها يجب أن تعطي لشركة التأمين صورة واقعية عن تعرضها للمخاطر السيبرانية بالإضافة للسيناريوهات المتوقعة وتأثيراتها حتى يتم تحويل هذه المعلومات إلى خطة عمل لإدارة المخاطر السيبرانية. (فطيمة، ٢٠٢٣م)

## الفصل الثالث

### منهجية الدراسة

## الفصل الثالث: منهجية الدراسة

### مقدمة

يتضمن هذا الجزء من أجزاء البحث على توضيح لخطوات وإجراءات البحث الميدانية مثل بيان مجتمع وعينة البحث، وأداة جمع المعلومات وكيفية بنائها، وإجراءات الصدق والثبات، والأساليب الإحصائية التي ستستخدم في معالجة وتحليل المعلومات. كما سيتم في هذا الفصل استعراض المنهجية والإجراءات المتبعة في الدراسة بشكل شامل. يتضمن ذلك تحديد المنهجية المستخدمة، وتعريف المجتمع المستهدف والعينة التي سيتم دراستها. كما سيتم تناول أدوات جمع البيانات من حيث إعدادها وطرق التحقق من صدقها وثباتها، بالإضافة إلى توضيح الأدوات والعمليات الإحصائية التي سيتم اعتمادها في تحليل البيانات، وذلك كما يلي:

### منهج الدراسة

اعتمد الباحث 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، من خلال الاعتماد على المنهج الوصفي لعرض الجوانب النظرية التي ترتبط بإدارة مخاطر الأمن السيبراني، كما سوف يعتمد الباحث في الجانب الكمي التحليلي على الاستبيان كأداة لجمع البيانات الأولية عن المشكلة محل الدراسة، للخروج بأهم النتائج والتوصيات التي ترتبط بالموضوع محل الدراسة.

## 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

- 1- الحدود الموضوعية: يركز البحث على إدارة مخاطر الأمن السيبراني في شركات التأمين، ولا يتناول مجالات أخرى من الأمن السيبراني خارج هذا القطاع.
- 2- الحدود المكانية: سيتم تطبيق الدراسة على أفرع وكاتب مؤسسة التأمين بالمملكة العربية السعودية.
- 3- 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 2025م.
- 4- 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.

## مجتمع وعينة البحث

يتألف مجتمع البحث من جميع المدراء الماليين وخبراء الأمن السيبراني وتكنولوجيا المعلومات بشركات التأمين

العاملة بالمملكة العربية السعودية، حيث بلغ عددهم (28) شركة مرخصة لمزاولة أنشطة التأمين. وقد تم اختيار عينة

البحث بطريقة عشوائية بسيطة ممثلة لمجتمع البحث بحجم (88) مبحوث (مدير مالي، وخبير تكنولوجيا المعلومات،

ومسئول إدارة المخاطر السيبرانية)، وتم توزيع (100) استبانة وتم استرداد (92) استبانة منها (88) صالحة و(4) غير

صالحة للتحليل.

## خصائص أفراد عينة البحث (المتغيرات الديموغرافية)

يتصف أفراد عينة البحث بعدد من الخصائص الوظيفية، والتي يتوقع الباحث وجود اتجاهات بالاستجابات

بناءً عليها، والتي تشمل الخصائص التالية:-

جدول رقم (1): خصائص أفراد عينة البحث

| المتغير الديموغرافي | الفئات                       | العدد | النسبة المئوية |
|---------------------|------------------------------|-------|----------------|
| الوظيفة             | الإدارة المالية              | 37    | 42.05%         |
|                     | إدارة المخاطر                | 11    | 12.50%         |
|                     | الأمن السيبراني              | 21    | 23.86%         |
|                     | نظم المعلومات                | 19    | 21.59%         |
| المؤهل العلمي       | دبلوم                        | 12    | 13.64%         |
|                     | بكالوريوس                    | 68    | 77.27%         |
|                     | ماجستير                      | 5     | 5.68%          |
|                     | دكتوراه                      | 3     | 3.41%          |
| عدد سنوات الخبرة    | أقل من خمس سنوات             | 22    | 25.00%         |
|                     | من خمسة إلى أقل من عشر سنوات | 48    | 54.55%         |
|                     | أكثر من عشر سنوات            | 18    | 20.45%         |
| الإجمالي            |                              | 88    | 100.00%        |

تشير النتائج إلى أن 42.05% من المشاركين يعملون في مجال الإدارة المالية، مما يعكس أهمية هذا القطاع في

سياق الدراسة. كما يتوزع المشاركون بين إدارة المخاطر (12.50%) والأمن السيبراني (23.86%) ونظم المعلومات

(21.59%). هذا التنوع يُظهر اهتمامًا واسعًا بالمجالات المتعلقة بالحوكمة وإدارة المخاطر. كما ترتفع نسبة الحاصلين

على بكالوريوس إلى 77.27%، مما يشير إلى أن معظم المشاركين يمتلكون خلفية أكاديمية قوية. بينما تظل النسب الأخرى للمؤهلات العليا مثل الماجستير (5.68%) والدكتوراه (3.41%) منخفضة، مما قد يدل على وجود فرصة لتحفيز المزيد من الأفراد ذوي المؤهلات العليا للدخول في هذه المجالات. وتظهر البيانات أن 54.55% من المشاركين لديهم خبرة تتراوح بين خمسة إلى أقل من عشر سنوات. بينما 25.00% من المشاركين لديهم خبرة أقل من خمس سنوات، و20.45% لديهم خبرة تزيد عن عشر سنوات. هذا التوزيع يعكس وجود مزيج جيد من الخبرات، مما يمكن أن يؤدي إلى تبادل المعرفة وتعزيز الممارسات الجيدة في مجالات العمل المختلفة.

#### أداة البحث

قام الباحث بتصميم أداة البحث الميداني، والمتمثلة في استبيان للتعرف دور إدارة المخاطر السيبرانية لشركات التأمين، والمتضمنة ثلاثة محاور، وتم وضع مجموعة من العبارات التي تُعبر عن كل محور وتُمثله. وتكونت الاستبانة في صورتها النهائية من (28) عبارة موزعة على ثلاثة محاور، المحور الأول يعكس محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني، وتشمل (9) عبارات. أما المحور الثاني فيشير إلى طبيعة ومحددات المخاطر السيبرانية بشركات التأمين، وشمل (8) عبارات. بينما المحور الثالث فيعكس مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين، وشمل (11) عبارة. وطلب الباحث من أفراد عينة الدراسة الإجابة على سلم ليكرت الخماسي لأحد الخيارات الآتية:-

- 1- موافق بشدة
- 2- موافق
- 3- محايد
- 4- غير موافق
- 5- غير موافق على الإطلاق

## ثبات أداة الدراسة

إن ثبات الأداة تشير إلى قدرة الأداة على إعطاء نفس النتائج إذا تم تكرار القياس على نفس الشخص عدة

مرات في نفس الظروف. وقد تم التأكد من ثبات الاستبانة بواسطة معامل الثبات ألفا كرونباخ في ضوء استجابات

مقياس ليكرت الخماسي. ويوضح الجدول التالي معامل الثبات لكل من المحاور الفرعية وإجمالي الاستبيان.

جدول رقم (2): معامل الثبات ألفا كرونباخ لكل من المحاور الفرعية وإجمالي الاستبيان

| الثبات | عدد العبارات | المحور                                                             |
|--------|--------------|--------------------------------------------------------------------|
| 0.874  | 9            | المحور الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني     |
| 0.883  | 8            | المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     |
| 0.649  | 11           | المحور الثالث: مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين |
| 0.913  | 28           | إجمالي الاستبيان                                                   |

يتضح من بيانات الجدول السابق أنّ إجمالي فقرات الاستبيان تتمتع بدرجة مرتفعة جداً من الثبات، حيث

بلغت قيمة الثبات (0.913)، بلغت قيمة الثبات للمحور الأول (0.874)، وبلغت قيمة الثبات في المحور الثاني (0.883)،

وكانت قيمة الثبات في المحور الثالث (0.649)، ويعدّ معامل ثبات ألفا كرونباخ المساوي 0.7 مقبولاً بشكل عام كأقل

قيمة مرغوبة للمعامل.

## إجراءات تطبيق الدراسة

لمحاولة الإجابة عن أسئلة الدراسة، اتبع الباحث الخطوات التالية:-

- 1- تم الاطلاع على العديد من الدراسات والبحوث السابقة في هذا المجال سواء كانت عربية أو أجنبية.
- 2- تم تحديد وإعداد وبناء أداة الدراسة وتجهيزها وهي الاستبانة، حيث احتوت الاستبانة في صورتها النهائية على ثلاثة أقسام: يحتوي القسم الأول على مقدمة تمهيدية، والقسم الثاني يحتوي على البيانات الأولية

للمستجيبين والتي تشمل على المتغيرات الديموغرافية، والقسم الثالث يتضمن (28) عبارة تعكس محاور

الاستبيان الثالث.

3- للحصول على بيانات مجتمع وعينة الدراسة، تم الحصول على تلك البيانات عن طريق إرسال رابط

للاستبيان الإلكتروني، ثم الحصول على الاستجابات من خلال ملف Excel.

4- قام الباحث بتوزيع أداة الاستبانة على أفراد عينة الدراسة خلال العام الدراسي 1447 هـ - 2025 م، عن

طريق نشر أداة الاستبانة وتوزيعها على جميع المستجيبين، وتم الرد (88).

5- تم رصد النتائج وتحليلها وتفسيرها وتقديم التوصيات.

#### أساليب التحليل الإحصائية

لتحقيق أهداف البحث وتحليل البيانات التي تم تجميعها، تم استخدام العديد من الأساليب الإحصائية

المناسبة باستخدام الحزم الإحصائية للعلوم الاجتماعية (SPSS). وذلك بعد ترميز وإدخال البيانات إلى الحاسب الآلي،

وتم تصميم الاستبانة وفق التدرج الخماسي لمقياس ليكرت (Likert)، وذلك لقياس مستوى استجابات أفراد عينة

الدراسة حول فقرات أداة الاستبانة، كما هو موضح في الجدول رقم (4):

جدول (3): درجات المقياس الخماسي لليكرت

| الاستجابات | موافق بشدة | موافق | محايد | غير موافق | غير موافق على الإطلاق |
|------------|------------|-------|-------|-----------|-----------------------|
| الدرجة     | 5          | 4     | 3     | 2         | 1                     |

وقد تم تقدير كل من درجة ممارسة أبعاد القيادة المستدامة وأبعاد الصحة التنظيمية، وفق المعاملات

الحسابية التالية، والجدول (5) يوضح ذلك:

$$10 - \text{المدى} = \text{أعلى درجة} - \text{أقل درجة} = 4$$

$$11 - \text{طول الفئة} = \text{المدى} \div \text{عدد الفئات} = 0.80$$

جدول (4): حدود متوسطات استجابات أفراد الدراسة وفقاً لفئات مقياس ليكرت الخماسي

| م | الفئة                 | من   | إلى         | حدود الفئة (متوسطات الاستجابات) |
|---|-----------------------|------|-------------|---------------------------------|
| 1 | موافق بشدة            | 4,20 | 5,00        |                                 |
| 2 | موافق                 | 3,40 | أقل من 4,20 |                                 |
| 3 | محايد                 | 2,60 | أقل من 3,40 |                                 |
| 4 | غير موافق             | 1,80 | أقل من 2,60 |                                 |
| 5 | غير موافق على الإطلاق | 1,00 | أقل من 1,80 |                                 |

المصدر: من إعداد الباحث

ولخدمة أغراض الدراسة وتحليل البيانات التي تم تجميعها من خلال أداة الدراسة في الجانب الميداني،

استخدمت عدد من الأساليب الإحصائية لمعرفة اتجاهات أفراد مجتمع الدراسة حول التساؤلات المطروحة، وذلك

باستخدام أساليب المعالجة الإحصائية التالية:

1- التكرارات والنسب المئوية للتعرف على الخصائص الشخصية والوظيفية لأفراد عينة الدراسة وتحديد

استجابات أفرادها تجاه فقرات المحاور الرئيسة التي تتضمنها أداة الدراسة.

2- المتوسط الحسابي "Mean" وذلك لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد عينة الدراسة عن المحاور

الرئيسة (متوسط العبارات)، كما تم ترتيب المحاور حسب أعلى متوسط حسابي.

3- الانحراف المعياري " Standard Deviation " للتعرف على مدى تجانس استجابات عينة الدراسة، وكذلك

انحراف استجابات أفراد عينة الدراسة لكل من فقرات متغيرات الدراسة، ولكل محور من المحاور الرئيسة عن متوسطها الحسابي.

4- معامل الارتباط بيرسون person Correlation لمعرفة درجة الارتباط بين فقرات الاستبانة والمحور الذي تنتهي إليه كل فقرة من الفقرات.

5- معامل ألفا كرونباخ ( Cronch'lph ) لاختبار مدى ثبات أداة الدراسة.

6- اختبار ت (T-test) لمعرفة مدى وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة حول محاور الاستبيان التي تعزى للمتغيرات ثنائية التصنيف.

7- اختبار تحليل التباين (ANOVA) لمعرفة مدى وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة حول محاور الاستبيان التي تعزى للمتغيرات غير الثنائية التصنيف.

#### صدق فقرات أداة الدراسة

تم قياس صدق الاتساق الداخلي لأداة الدراسة باستخدام معامل ارتباط بيرسون لكل محور، وذلك من خلال حساب الارتباط بين كل عبارة والدرجة الكلية للمحور التابع له. يوضح الجدول أدناه نتائج معاملات الارتباط:-

جدول رقم (5): صدق الاتساق الداخلي لمحاور الدراسة

| المحاور       | رقم العبارة | معامل الارتباط | رقم العبارة | معامل الارتباط |
|---------------|-------------|----------------|-------------|----------------|
| المحور الأول  | 1           | 0.772          | 6           | 0.834          |
|               | 2           | 0.653          | 7           | 0.783          |
|               | 3           | 0.831          | 8           | 0.755          |
|               | 4           | 0.714          | 9           | 0.678          |
|               | 5           | 0.726          |             |                |
| المحور الثاني | 1           | 0.682          | 5           | 0.697          |
|               | 2           | 0.79           | 6           | 0.817          |
|               | 3           | 0.724          | 7           | 0.614          |

|       |    |       |   |               |
|-------|----|-------|---|---------------|
| 0.671 | 8  | 0.851 | 4 | المحور الثالث |
| 0.747 | 7  | 0.659 | 1 |               |
| 0.667 | 8  | 0.731 | 2 |               |
| 0.647 | 9  | 0.808 | 3 |               |
| 0.617 | 10 | 0.777 | 4 |               |
| 0.692 | 11 | 0.818 | 5 |               |
|       |    | 0.717 | 6 |               |

يتضح من الجدول أن جميع معاملات الارتباط بين كل فقرة ودرجة المحور الأول جاءت مرتفعة وتراوح بين

(0.653 – 0.834)، ودرجة المحور الثاني جاءت مرتفعة وتراوح بين (0.614 – 0.817)، ودرجة المحور الثالث جاءت

مرتفعة وتراوح بين (0.617 – 0.818). كما يتضح أن جميع قيم المحاور موجبة وجميعها دالة عند مستوى دلالة

إحصائية 1% مما يشير إلى أن محاور الدراسة تمتاز بصدق الاتساق الداخلي وأن فقراتها ترتبط بالمحاور بصورة كبيرة

وبالتالي فهي تقيس ما صممت الاستبانة من أجله من أهداف بحثية.

#### ثبات الاستبانة (Reliability)

تم الاعتماد على معامل ألفا كرونباخ لكل من الاستبيان ككل وكذلك المحاور الفرعية للاستبيان. ويقاس معامل

المصدقية ألفا كرونباخ درجة الاعتمادية على نتائج صدق وثبات النتائج، بمعنى أن الاستبيان يقدم نفس النتائج حتى

ولو تم إعادة استكمال النتائج مرة أخرى من نفس العينة، وهو ما يقدم درجة صدق وثبات نتائج الاستبيان.

جدول رقم (6): معامل الثبات ألفا كرونباخ لمحاور الاستبيان

Scale: ALL VARIABLES

#### Case Processing Summary

|                             | N  | %     |
|-----------------------------|----|-------|
| Valid                       | 88 | 100.0 |
| Cases Excluded <sup>a</sup> | 0  | .0    |
| Total                       | 88 | 100.0 |

a. Listwise deletion based on all variables in the procedure.

#### Reliability Statistics

| المحاور        | Cronbach's Alpha <sup>a</sup> | N of Items |
|----------------|-------------------------------|------------|
| الأول          | .812                          | 9          |
| الثاني         | .921                          | 8          |
| الثالث         | .935                          | 11         |
| كامل الاستبيان | .949                          | 28         |

من خلال الجدول السابق يتضح أن المستجيبين قد بلغ عددهم 88 مستجيب، وقد شمل الاستبيان عدد 28

فقرة، وقد بلغت قيمة معامل الثبات 949. وهو معامل مرتفع يدل على صدق وثبات الاستجابات الخاصة بالاستبيان.

وهو ما يقدم لنا مؤشر في امكانية الاستمرار في تحليل فقرات الاستبيان كنتيجة لارتفاع قيمة ثباته.

## نتائج الدراسة ومناقشتها وتفسيرها

هذا الجزء من أجزاء البحث يتناول عرض نتائج الدراسة الميدانية ومناقشتها وتفسيرها من خلال عرض إجابات أفراد عينة الدراسة على فقرات أداة الاستبانة، وذلك من خلال الإجابة على تساؤلات الدراسة على النحو التالي:

### البعد الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني

للتعرف على محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني (المحور الأول)، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات مفردات الدراسة، وجاءت النتائج كما يلي:-

جدول رقم (7): محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني (المحور الأول)

| م                          | الفقرات                                                                                                   | المتوسط الحسابي | الانحراف المعياري |
|----------------------------|-----------------------------------------------------------------------------------------------------------|-----------------|-------------------|
| 1                          | تدرج إدارة استثمارات تكنولوجيا المعلومات وتطويرها وإقرارها ضمن موازنة تكنولوجيا المعلومات للقطاع التأميني | 4.10            | 0.80              |
| 2                          | يوجد تقييم مستمر ومتتالي لاستراتيجية القطاع التأميني المتعلقة بأساليب تكنولوجيا المعلومات.                | 3.86            | 0.78              |
| 3                          | تنظيم وهيكلية تكنولوجيا المعلومات يتم وفق خطة القطاع التأميني المتطورة.                                   | 4.07            | 0.83              |
| 4                          | تتغير خطة تكنولوجيا المعلومات في قطاع التأمين باستمرار.                                                   | 3.95            | 0.84              |
| 5                          | لا يتم السماح لغير المصرح لهم بالدخول إلى برامج القطاع التأميني المختلفة.                                 | 3.97            | 0.87              |
| 6                          | تأكيد الشركات على أن مخاطر تكنولوجيا المعلومات يتم إدارتها بكفاءة.                                        | 4.03            | 0.76              |
| 7                          | توجد دورات مستمرة للعاملين بقطاع التأمين على تكنولوجيا المعلومات.                                         | 4.00            | 0.79              |
| 8                          | توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدارة القطاع.                                                  | 4.07            | 0.72              |
| 9                          | فاعلية السياسة الداخلية في قطاع التأمين بشأن تفعيل آليات تكنولوجيا المعلومات.                             | 4.12            | 0.85              |
| المتوسط العام للمحور الأول |                                                                                                           | 4.03            | 0.77              |

يوضح الجدول السابق قيمة المتوسط الحسابي والانحراف المعياري لكل من أسئلة المحور الأول من

الاستبيان، وكذلك اجمالي المحور الأول، كما يوضح الجدول نتائج استبيان يتناول تقييم إدارة استثمارات تكنولوجيا

المعلومات في القطاع التأميني، مع التركيز على عدة محاور رئيسية. تم حساب المتوسطات والانحرافات المعيارية لكل

فقرة، مما يوفر رؤية قيمة حول مستوى التقبل والفعالية في تطبيق تكنولوجيا المعلومات.

تدرج إدارة استثمارات تكنولوجيا المعلومات، بلغ متوسط هذه الفقرة 4.10 مع انحراف معياري قدره 0.80، مما يشير إلى أن المشاركين يعتبرون أن إدارة استثمارات تكنولوجيا المعلومات وتطويرها وإقرارها ضمن الموازنة أمر مهم للغاية. هذا المستوى العالي من التقييم يعكس التزام القطاع التأميني بتخصيص الموارد اللازمة لتكنولوجيا المعلومات، مما يسهم في تحسين كفاءة العمليات. تقييم استراتيجية تكنولوجيا المعلومات، بلغ متوسط هذه الفقرة 3.86 مع انحراف معياري قدره 0.78. تشير هذه القيمة إلى وجود تقييم مستمر لاستراتيجية تكنولوجيا المعلومات، ولكن بشكل أقل قوة مقارنة بالفقرات الأخرى. قد يعني ذلك أن هناك جهودًا مستمرة للتقييم، إلا أن المشاركين يرون أن هناك مجالًا للتحسين في كيفية تنفيذ هذه التقييمات بشكل دوري.

تنظيم وهيكلية تكنولوجيا المعلومات، متوسط هذه الفقرة 4.07 مع انحراف معياري 0.83، مما يدل على أن تنظيم وهيكلية تكنولوجيا المعلومات يتم وفق خطة متطورة. يشير هذا إلى أن القطاع التأميني يتبنى منهجيات استراتيجية في تنظيم تكنولوجيا المعلومات، مما يساعد في تحقيق الأهداف العامة. تغيير خطة تكنولوجيا المعلومات، بلغ متوسط هذه الفقرة 3.95 مع انحراف معياري 0.84، مما يعني أن المشاركين يرون أن خطة تكنولوجيا المعلومات تتغير باستمرار. هذا يشير إلى أن القطاع التأميني يواجه تحديات في التكيف مع التغيرات السريعة في تكنولوجيا المعلومات، مما يتطلب مرونة أكبر في الخطط.

الدخول المصرح به فقط، متوسط هذه الفقرة 3.97 مع انحراف معياري 0.87، مما يدل على أن هناك اهتمامًا كبيرًا بالأمان وضمان عدم دخول غير المصرح لهم إلى برامج القطاع التأميني. يعكس هذا التقييم أهمية حماية البيانات والمعلومات في القطاع. إدارة مخاطر تكنولوجيا المعلومات، بلغ متوسط هذه الفقرة 4.03 مع انحراف معياري 0.76، مما يشير إلى أن الشركات تؤكد على كفاءة إدارة مخاطر تكنولوجيا المعلومات. يعكس هذا الالتزام بوجود

استراتيجيات فعالة لإدارة المخاطر، مما يعزز من الأمان السيبراني. دورات تدريبية للعاملين، متوسط هذه الفقرة 4.00

مع انحراف معياري 0.79، مما يدل على وجود دورات مستمرة للعاملين في قطاع التأمين على تكنولوجيا المعلومات. يشير

هذا إلى أهمية تدريب العاملين وتمكينهم من استخدام التقنيات الحديثة بكفاءة.

لجنة تكنولوجيا المعلومات، بلغ متوسط هذه الفقرة 4.07 مع انحراف معياري 0.72، مما يشير إلى وجود لجنة

مختصة لتكنولوجيا المعلومات تابعة لمجلس إدارة القطاع. يشير ذلك إلى أن هناك هيكلًا تنظيميًا داعمًا لتكنولوجيا

المعلومات، مما يعزز من اتخاذ القرارات الاستراتيجية. فاعلية السياسة الداخلية، متوسط هذه الفقرة 4.12 مع

انحراف معياري 0.85، مما يدل على أن المشاركين يرون أن السياسة الداخلية في قطاع التأمين فعالة بشأن تفعيل

آليات تكنولوجيا المعلومات. هذا يشير إلى وجود إطار عمل قوي لدعم استخدام تكنولوجيا المعلومات. بلغ المتوسط

العام لهذا المحور 4.03 مع انحراف معياري 0.77، مما يدل على مستوى إيجابي عام في تقييم المشاركين لإدارة استثمارات

تكنولوجيا المعلومات في القطاع التأميني.

تعكس هذه النتائج التزام القطاع بالتطوير المستمر واستراتيجيات الأمان، مع وجود بعض المجالات التي

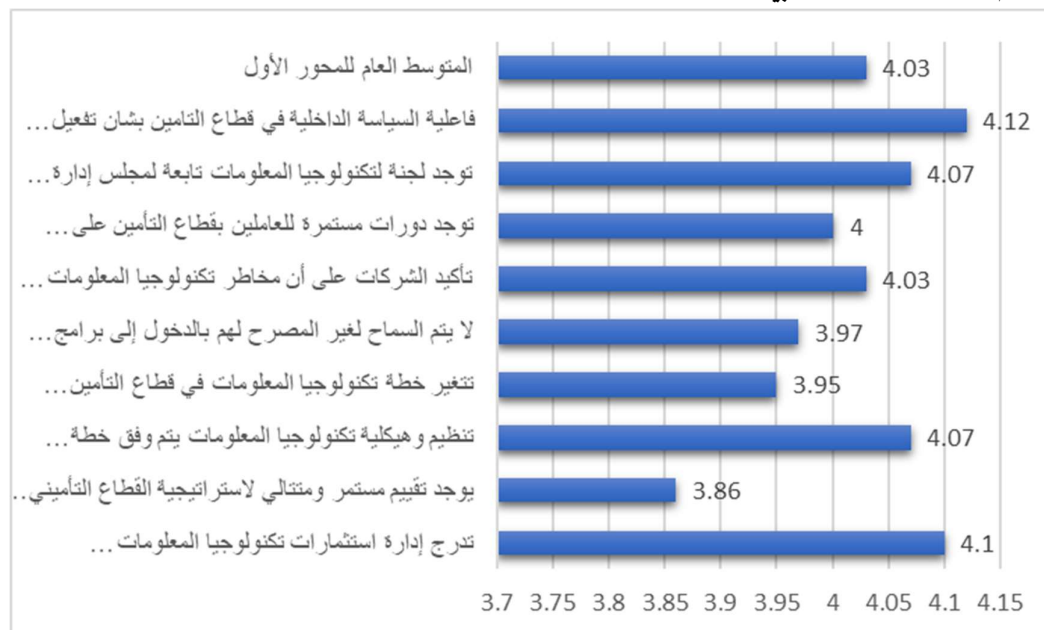
تحتاج إلى تحسين، مثل تقييم الاستراتيجيات وتطبيق التغييرات بمرونة أكبر. تشير النتائج إلى أن القطاع التأميني يسعى

بشكل جاد لتعزيز استثماراته في تكنولوجيا المعلومات من خلال خطط واضحة وتقييمات مستمرة. ومع ذلك، يجب

على القطاع التركيز على تحسين مرونة خطط تكنولوجيا المعلومات وضمان التدريب المستمر للعاملين لتعزيز الكفاءة

والأمان.

شكل رقم (1): المتوسط الحسابي والانحراف للمحور الأول محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني



## ثانياً: المحور الثاني (طبيعة ومحددات المخاطر السيبرانية بشركات التأمين)

يعكس المحور الثاني طبيعة ومحددات المخاطر السيبرانية بشركات التأمين. ويوضح الجدول التالي متوسط

استجابات عينة الدراسة تجاه فقرات المحور الثاني وكذلك قيمة الانحراف المعياري.

جدول رقم (8): المتوسط الحسابي والانحراف للمحور الثاني طبيعة ومحددات المخاطر السيبرانية بشركات التأمين

| الفقرات                                                                                                 | Mean | Std. Deviation |
|---------------------------------------------------------------------------------------------------------|------|----------------|
| 1 يقوم القطاع التأميني بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية.                | 4.12 | 0.87           |
| 2 يقوم القطاع التأميني بضبط معايير الأنشطة التأمينية الإلكترونية.                                       | 4.58 | 0.50           |
| 3 يقوم القطاع التأميني بتحسين خدمات التأمين الإلكترونية لإرضاء العملاء.                                 | 3.44 | 0.50           |
| 4 يقوم القطاع التأميني بالإشراف على مخاطر تكنولوجيا المعلومات وإدارتها بكفاءة.                          | 3.64 | 0.50           |
| 5 يقوم القطاع التأميني بإدارة التهديدات والتوجيهات المتعلقة بالمخاطر الإلكترونية.                       | 4.07 | 0.76           |
| 6 يقوم القطاع التأميني بالتوسع في تقديم الخدمات والمنتجات التأمينية لمعرفة السوق والتحقق من صحة ضمانات. | 3.54 | 0.50           |
| 7 يقوم القطاع التأميني ببيان المعلومات والحفاظ على خصوصية البيانات.                                     | 3.93 | 0.78           |
| 8 يقوم التأمين بتعزيز حماية المؤسسة من المجموعات الإلكترونية المهددة.                                   | 3.53 | 0.50           |
| المتوسط العام للمحور الثاني                                                                             | 3.85 | 0.20           |

يوضح الجدول السابق المتوسط المرجح لاستجابات عينة الدراسة نحو اسئلة الاستبيان. حيث جاءت اغلب

الفقرات ذات متوسط مرتفع حيث أن قيمة المتوسط لم تقل لاي من فقرات الاستبيان عن 3.6 أما المتوسط العام

للمحور فقد بلغ 3.85 باتجاه مرتفع. يوضح الجدول نتائج استبيان يتعلق بتقييم العمليات الإلكترونية وإدارة المخاطر

في القطاع التأميني. يتم قياس كل فقرة من خلال المتوسطات والانحرافات المعيارية، مما يمكننا من فهم مستوى

الفعالية والالتزام في تنفيذ تكنولوجيا المعلومات .

صحة المعاملات والمسؤولية، بلغ متوسط هذه الفقرة 4.12 مع انحراف معياري قدره 0.87، مما يشير إلى أن

المشاركين يشعرون بأن القطاع التأميني يؤكد على صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية. هذا

الرقم يعكس مستوى عالٍ من الثقة في العمليات الإلكترونية، مما يعزز من مصداقية القطاع في التعاملات. ضبط

معايير الأنشطة الإلكترونية، تظهر الفقرة الثانية متوسطاً قدره 4.58 مع انحراف معياري 0.50، مما يدل على أن هناك

التزاماً قوياً بضبط معايير الأنشطة التأمينية الإلكترونية. تعتبر هذه النتيجة إيجابية للغاية، حيث تشير إلى أن القطاع

التأميني يأخذ معايير الجودة والتحكم بشكل جاد، مما يعزز من فعالية العمليات. تحسين خدمات التأمين الإلكترونية،

بلغ متوسط هذه الفقرة 3.44 مع انحراف معياري 0.50، مما يدل على أن المشاركين يرون أن هناك حاجة لتحسين

خدمات التأمين الإلكترونية لإرضاء العملاء.

هذا الرقم يشير إلى وجود مجال كبير للتحسين، مما يتطلب استراتيجيات أكثر قوة لتحسين تجربة العملاء.

الإشراف على مخاطر تكنولوجيا المعلومات، متوسط هذه الفقرة هو 3.64 مع انحراف معياري 0.50، مما يعني أن

المشاركين يعتبرون أن الإشراف على مخاطر تكنولوجيا المعلومات وإدارتها يتم بشكل كافٍ، لكن ليس بشكل مثالي. يشير

هذا إلى أهمية تعزيز الجهود في إدارة المخاطر لضمان الأمان في العمليات الإلكترونية. إدارة التهديدات الإلكترونية، بلغ

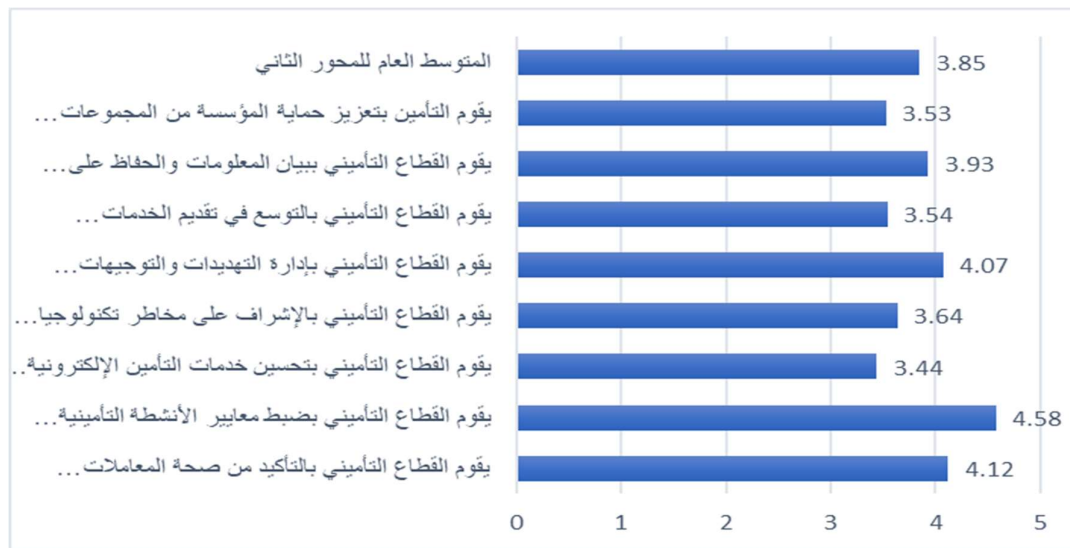
متوسط هذه الفقرة 4.07 مع انحراف معياري 0.76، مما يعكس أن القطاع التأميني يدير التهديدات والتوجهات

المتعلقة بالمخاطر الإلكترونية بشكل فعال. هذا يعكس التزاماً بحماية المعلومات والبيانات من المخاطر المحتملة.

التوسع في تقديم الخدمات، متوسط هذه الفقرة هو 3.54 مع انحراف معياري 0.50، مما يدل على أن هناك رغبة في التوسع في تقديم الخدمات والمنتجات التأمينية. ومع ذلك، فإن هذا الرقم يشير إلى أن هناك حاجة لمزيد من الجهود في هذا الاتجاه. حماية المعلومات وخصوصيتها، بلغ متوسط هذه الفقرة 3.93 مع انحراف معياري 0.78، مما يدل على أن المشاركين يرون أن القطاع التأميني يبذل جهودًا للحفاظ على خصوصية البيانات. هذا مهم جدًا في ظل المخاطر المتزايدة المتعلقة بالأمان السيبراني.

تعزيز الحماية من المخاطر الإلكترونية، متوسط هذه الفقرة 3.53 مع انحراف معياري 0.50، مما يدل على أن هناك جهودًا لتعزيز حماية المؤسسة من المجموعات الإلكترونية المهددة، لكن لا تزال هناك حاجة لتحسين هذه الجهود. بلغ المتوسط العام لهذا المحور 3.85 مع انحراف معياري 0.20، مما يدل على مستوى إيجابي عام في تقييم المشاركين للعمليات الإلكترونية وإدارة المخاطر في القطاع التأميني. يشير هذا الرقم إلى أن هناك التزامًا قويًا بالتحسين، ولكن لا يزال هناك مجال للتحسين خاصة في تحسين خدمات التأمين الإلكترونية وإدارة المخاطر. تشير النتائج إلى أن القطاع التأميني يبذل جهودًا ملحوظة في تأكيد صحة المعاملات وضبط المعايير، لكن هناك حاجة واضحة لتحسين خدمات التأمين الإلكترونية وإدارة المخاطر. يجب أن تركز الاستراتيجيات المستقبلية على تعزيز تجربة العملاء وحماية البيانات، مما يساهم في تعزيز الثقة في القطاع التأميني.

شكل رقم (2): المتوسط الحسابي والانحراف للمحور الثاني طبيعة ومحددات المخاطر السيبرانية بشركات التأمين



### ثانياً: المحور الثالث (مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين)

يعكس المحور الثالث مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين. ويوضح الجدول التالي متوسط

استجابات عينة الدراسة تجاه فقرات المحور الثاني وكذلك قيمة الانحراف المعياري.

جدول رقم (9): المتوسط الحسابي والانحراف للمحور الثالث مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين

| م  | الفقرات                                                                                                                       | Mean | Std. Deviation |
|----|-------------------------------------------------------------------------------------------------------------------------------|------|----------------|
| 1  | توفر إدارة المخطر السيبرانية تقييم المخاطر السيبرانية بصورة دورية.                                                            | 3.93 | 0.5            |
| 2  | تعمل إدارة المخطر السيبرانية على الحد من مخاطر تكنولوجيا المعلومات وعدم تكرارها.                                              | 3.53 | 0.78           |
| 3  | تحسن إدارة المخطر السيبرانية أداء المخاطر بالتأمين على بنية المعلومات.                                                        | 3.74 | 0.5            |
| 4  | تسهم إدارة المخطر السيبرانية في تعزيز الأمان للمعلومات والمخاطر السيبرانية.                                                   | 3.9  | 0.5            |
| 5  | تعمل إدارة المخطر السيبرانية على تطوير نظم الحماية من المخاطر السيبرانية.                                                     | 3.94 | 0.86           |
| 6  | توفر إدارة المخطر السيبرانية الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات.                                         | 4.12 | 0.81           |
| 7  | توفر إدارة المخطر السيبرانية إجراء اختبارات دورية للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية ضد مخاطر الأمن السيبراني. | 4.58 | 0.87           |
| 8  | تحقق إدارة المخطر السيبرانية وجود قسم مخصص لإدارة المخاطر ضد المخاطر السيبرانية.                                              | 3.44 | 0.5            |
| 9  | تعمل إدارة المخطر السيبرانية على المرونة اللازمة لزيادة حماية البيانات.                                                       | 3.64 | 0.5            |
| 10 | توفر إدارة المخطر السيبرانية تحديث وتطوير نظم الحماية من المخاطر السيبرانية بشكل دوري                                         | 4.07 | 0.5            |
| 11 | توفر إدارة المخطر السيبرانية تدريب العاملين في تكنولوجيا المعلومات على التصدي للمخاطر السيبرانية.                             | 3.54 | 0.76           |
|    | المتوسط العام للمحور الثالث                                                                                                   | 3.74 | 0.26           |

يوضح الجدول السابق المتوسط المرجح لاستجابات عينة الدراسة نحو أسئلة الاستبيان عن أداء العاملين

وعلاقتها بالبرامج التدريبية. حيث جاءت اغلب الفقرات ذات متوسط مرتفع حيث أن قيمة المتوسط لم تقل لأي من

فقرات الاستبيان عن 3.6 أما المتوسط العام للمحور فقد بلغ 3.74 باتجاه مرتفع. فيما يتعلق بتقييم الفقرات للفقرة

الأولى تقييم المخاطر السيبرانية دوريًا، بلغ متوسط هذه الفقرة 3.93 مع انحراف معياري قدره 0.5، مما يشير إلى أن المشاركين يرون أن إدارة المخاطر السيبرانية توفر تقييمًا دوريًا للمخاطر. هذا يعكس التزام القطاع بالتقييم المستمر، مما يعزز من قدرة المؤسسات على التعرف على التهديدات المحتملة. الحد من مخاطر تكنولوجيا المعلومات، تظهر الفقرة الثانية متوسطًا قدره 3.53 مع انحراف معياري 0.78، مما يدل على أن إدارة المخاطر السيبرانية تعمل بفعالية على الحد من مخاطر تكنولوجيا المعلومات.

تعكس هذه النتيجة التزامًا قويًا بإدارة المخاطر، مما يعزز من الأمان السيبراني. تحسين أداء المخاطر، بلغ متوسط هذه الفقرة 3.74 مع انحراف معياري 0.50، مما يدل على أن المشاركين يرون أن إدارة المخاطر السيبرانية تحتاج إلى تحسين الأداء من خلال التأمين على بنية المعلومات. هذا الرقم يشير إلى وجود مجال للتحسين، مما يتطلب استراتيجيات أكثر فاعلية. تعزيز الأمان للمعلومات، متوسط هذه الفقرة هو 3.9 مع انحراف معياري 0.86، مما يعني أن المشاركين يعتبرون أن إدارة المخاطر السيبرانية تساهم في تعزيز الأمان للمعلومات. ولكن مستوى التقييم في هذه الفقرة يشير إلى الحاجة لمزيد من الجهود في هذا الاتجاه. تطوير نظم الحماية، بلغ متوسط هذه الفقرة 3.94 مع انحراف معياري 0.5، مما يعكس أن إدارة المخاطر السيبرانية تعمل على تطوير نظم الحماية بشكل فعال. هذا يعكس التزامًا بالاستجابة للتحديات المتزايدة في مجال الأمن السيبراني.

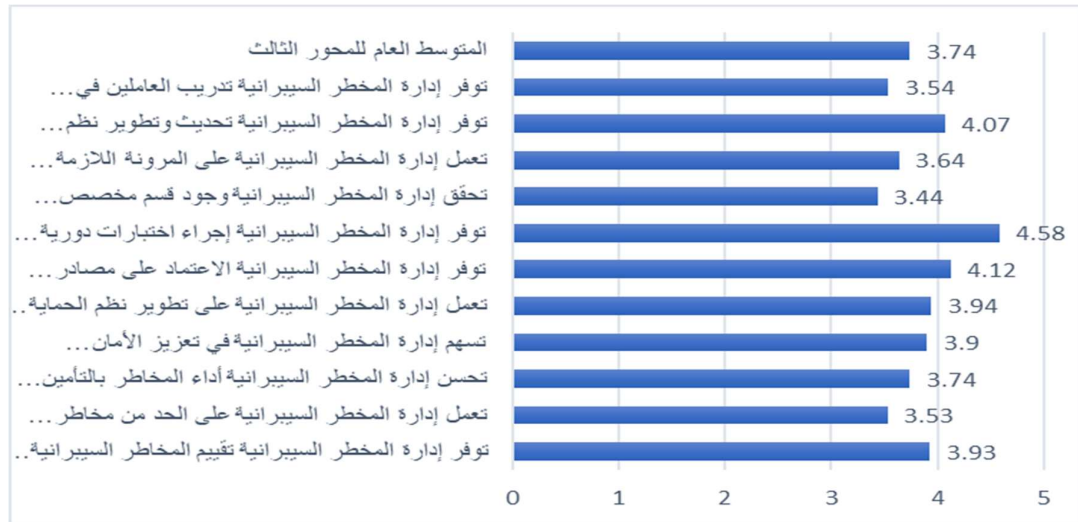
الاعتماد على مصادر مرخصة، متوسط هذه الفقرة هو 4.12 مع انحراف معياري 0.81، مما يدل على أن هناك حاجة لتحسين الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات. هذا يشير إلى أهمية تقييم أدوات الأمان المستخدمة في القطاع. إجراء اختبارات دورية، بلغ متوسط هذه الفقرة 4.58 مع انحراف معياري 0.87، مما يدل

على أن إدارة المخاطر السيبرانية توفر اختبارات دورية للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية. هذا يشير إلى وجود جهود جيدة، ولكن لا تزال هناك حاجة لتعزيز هذه الممارسات.

وجود قسم مخصص لإدارة المخاطر، متوسط هذه الفقرة 3.44 مع انحراف معياري 0.50، مما يدل على أن وجود قسم مخصص لإدارة المخاطر ضد المخاطر السيبرانية ليس قويًا بما فيه الكفاية. هذا يشير إلى أهمية تعزيز الهيكل التنظيمي لدعم إدارة المخاطر. المرونة اللازمة لحماية البيانات، بلغ متوسط هذه الفقرة 3.64 مع انحراف معياري 0.50، مما يدل على أن هناك حاجة للمرونة في استراتيجيات حماية البيانات. تشير هذه النتيجة إلى أهمية التكيف مع التغيرات السريعة في بيئة التهديدات. تحديث نظم الحماية، متوسط هذه الفقرة 4.07 مع انحراف معياري 0.5، مما يدل على أن إدارة المخاطر السيبرانية توفر تحديثات دورية لنظم الحماية. هذا يعكس التزامًا بتحسين الأمان السيبراني باستمرار.

تدريب العاملين على التصدي للمخاطر، بلغ متوسط هذه الفقرة 3.54 مع انحراف معياري 0.76، مما يشير إلى أن إدارة المخاطر السيبرانية توفر تدريبًا للعاملين في تكنولوجيا المعلومات. هذا مهم جدًا في تعزيز الوعي الأمني والقدرة على التصدي للتهديدات. بلغ المتوسط العام لهذا المحور 3.74 مع انحراف معياري 0.26، مما يدل على مستوى إيجابي عام في تقييم المشاركين لإدارة المخاطر السيبرانية. يشير هذا الرقم إلى أن هناك التزامًا قويًا بالتطوير والتحسين، لكن لا يزال هناك مجالات تحتاج إلى تحسين، مثل تعزيز الأمان وتحسين الأداء. تشير النتائج إلى أن إدارة المخاطر السيبرانية في القطاع التأميني تعمل بشكل جيد على تقييم المخاطر وتطوير نظم الحماية، لكنها تحتاج إلى المزيد من الجهود في مجالات تحسين الأداء وتوفير هيكل تنظيمي قوي لدعم إدارة المخاطر. التركيز على تدريب العاملين وتحديث الأنظمة بشكل دوري سيكون له تأثير إيجابي في تعزيز الأمان السيبراني.

شكل رقم (3): المتوسط الحسابي والانحراف للمحور الثالث مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين



## معنوية الفروق في اتجاهات المستجيبين تعزى للمتغيرات الديموغرافية

### الفئة الوظيفية

تم الاعتماد على اختبار تحليل التباين لفحص مدى وجود اختلافات معنوية تجاه تطبيق إدارة المخاطر

السيبرانية بشركات التأمين، والجدول التالي يوضح مخرجات التحليل.

جدول رقم (10): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً للفئة الوظيفية

| ANOVA                                                              |                | Sum of Squares | df    | Mean Square | F    | Sig. |
|--------------------------------------------------------------------|----------------|----------------|-------|-------------|------|------|
| المحور الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني     | Between Groups | 2.89           | 6.00  | 0.48        | 0.86 | 0.00 |
|                                                                    | Within Groups  | 45.98          | 82.00 | 0.56        |      |      |
|                                                                    | Total          | 48.87          | 88.00 |             |      |      |
|                                                                    |                |                |       |             |      |      |
| المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     | Between Groups | 4.06           | 6.00  | 0.68        | 0.82 | 0.00 |
|                                                                    | Within Groups  | 67.98          | 82.00 | 0.83        |      |      |
|                                                                    | Total          | 72.04          | 88.00 |             |      |      |
|                                                                    |                |                |       |             |      |      |
| المحور الثالث: مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين | Between Groups | 2.52           | 6.00  | 0.42        | 1.05 | 0.00 |
|                                                                    | Within Groups  | 32.84          | 82.00 | 0.40        |      |      |
|                                                                    | Total          | 35.36          | 88.00 |             |      |      |
|                                                                    |                |                |       |             |      |      |
| اجمالي الاستبيان                                                   | Between Groups | 2.55           | 6.00  | 0.43        | 0.91 | 0.00 |
|                                                                    | Within Groups  | 38.16          | 82.00 | 0.47        |      |      |
|                                                                    | Total          | 40.71          | 88.00 |             |      |      |
|                                                                    |                |                |       |             |      |      |

من خلال الجدول يتضح وجود فروق في الاستجابات تعزى لمتغير الفئة الوظيفية عند مستوى دلالة 5%.

حيث نجد أن قيمة احصائي الاختبار (Sig) أقل من مستوى المعنوية المستخدم في الاختبار 5%، لجميع ابعاد

الاستبيان. وبالتالي فإن متغير الفئة الوظيفية لم يؤثر في الاستجابات. ومن خلال الرجوع لقيم المتوسطات المرجحة

للفئات الوظيفية، نجد أن العاملين بكل من إدارة الأمن السيبراني ونظم المعلومات كان لهم أكبر توجه تجاه تطبيق

إدارة المخاطر السيبرانية، ثم العاملين بإدارة المخاطر، وكان أقل متوسط مرجح للعاملين بالإدارة المالية. وبالتالي فإن

الفروق المعنوية كانت لصالح كل من العاملين بإدارة الأمن السيبراني ونظم المعلومات لتطبيق إجراءات إدارة المخاطر

بشركات العينة.

### المؤهل العلمي

تم الاعتماد على اختبار تحليل التباين لفحص مدى وجود اختلافات معنوية للمستجيبين ترجع لمتغير المؤهل

العلمي، والجدول التالي يوضح مخرجات التحليل.

جدول رقم (11): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً للمستوى التعليمي

|                                                                    |                | ANOVA          |       |             |       |      |
|--------------------------------------------------------------------|----------------|----------------|-------|-------------|-------|------|
|                                                                    |                | Sum of Squares | df    | Mean Square | F     | Sig. |
| المحور الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني     | Between Groups | 2.097          | 6.00  | 1.048       | 2.347 | .106 |
|                                                                    | Within Groups  | 22.336         | 82.00 | .447        |       |      |
|                                                                    | Total          | 24.433         | 88.00 |             |       |      |
| المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     | Between Groups | .729           | 6.00  | .365        | .517  | .600 |
|                                                                    | Within Groups  | 35.290         | 82.00 | .706        |       |      |
|                                                                    | Total          | 36.019         | 88.00 |             |       |      |
| المحور الثالث: مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين | Between Groups | .329           | 6.00  | .164        | .473  | .626 |
|                                                                    | Within Groups  | 17.351         | 82.00 | .347        |       |      |
|                                                                    | Total          | 17.679         | 88.00 |             |       |      |
| اجمالي الاستبيان                                                   | Between Groups | .773           | 6.00  | .387        | .987  | .380 |
|                                                                    | Within Groups  | 19.582         | 82.00 | .392        |       |      |
|                                                                    | Total          | 20.356         | 88.00 |             |       |      |

من خلال الجدول يتضح عدم وجود فروق في الاستجابات تعزى لمتغير المؤهل العلمي عند مستوى دلالة 5%.

حيث نجد أن قيمة احصائي الاختبار (Sig) أكبر من مستوى المعنوية المستخدم في الاختبار 5%، لجميع ابعاد

الاستبيان. وبالتالي فإن متغير المؤهل العلمي لم يؤثر في الاستجابات.

## عدد سنوات الخبرة

تم الاعتماد على اختبار تحليل التباين لفحص مدى وجود اختلافات معنوية تجاه تطبيق إدارة المخاطر

السيبرانية بشركات التأمين، والجدول التالي يوضح مخرجات التحليل.

جدول رقم (12): اختبار تحليل التباين (ANOVA) لاختبار معنوية الفروق وفقاً لعدد سنوات الخبرة

|                                                                    |                | ANOVA          |       |             |       |
|--------------------------------------------------------------------|----------------|----------------|-------|-------------|-------|
|                                                                    |                | Sum of Squares | df    | Mean Square | F     |
| المحور الأول: محددات ومعوقات تطبيق إدارة مخاطر الأمن السيبراني     | Between Groups | 1.443          | 6.00  | .481        | 1.025 |
|                                                                    | Within Groups  | 22.990         | 82.00 | .469        |       |
|                                                                    | Total          | 24.433         | 88.00 |             |       |
| المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بشركات التأمين     | Between Groups | 2.030          | 6.00  | .677        | .975  |
|                                                                    | Within Groups  | 33.989         | 82.00 | .694        |       |
|                                                                    | Total          | 36.019         | 88.00 |             |       |
| المحور الثالث: مدى مساهمة إدارة المخاطر السيبرانية في قطاع التأمين | Between Groups | 1.258          | 6.00  | .419        | 1.251 |
|                                                                    | Within Groups  | 16.421         | 82.00 | .335        |       |
|                                                                    | Total          | 17.679         | 88.00 |             |       |
| اجمالي الاستبيان                                                   | Between Groups | 1.276          | 6.00  | .425        | 1.092 |
|                                                                    | Within Groups  | 19.080         | 82.00 | .389        |       |
|                                                                    | Total          | 20.356         | 88.00 |             |       |

من خلال الجدول يتضح عدم وجود فروق في الاستجابات تعزى لمتغير عدد سنوات الخبرة عند مستوى دلالة

5%. حيث نجد أن قيمة احصائي الاختبار (Sig) أكبر من مستوى المعنوية المستخدم في الاختبار 5%، لجميع ابعاد

الاستبيان. وبالتالي فإن متغير عدد سنوات الخبرة لم يؤثر في الاستجابات.

## الخاتمة

تُسلط هذه الدراسة الضوء على الأهمية المتزايدة لإدارة مخاطر الأمن السيبراني في قطاع التأمين، الذي يواجه تحديات متزايدة نتيجة لارتفاع عدد الهجمات السيبرانية وانتهاكات البيانات. من خلال تقييم فعالية استراتيجيات إدارة المخاطر وتحديد النقاط القابلة للتحسين، تبرز الدراسة التزام القطاع بتعزيز الأمان وزيادة الكفاءة التشغيلية. تشير النتائج إلى وجود مستوى إيجابي في تقييم إدارة استثمارات تكنولوجيا المعلومات، مع الحاجة الملحة لتعزيز برامج التدريب وتطوير الهيكل التنظيمي لدعم إدارة المخاطر. كما تم التعرف على أهمية تحديث الأنظمة بشكل دوري لضمان التكيف مع التغيرات المستمرة في بيئة التهديدات. توصي الدراسة بضرورة التركيز على تحسين تجربة العملاء وتعزيز الوعي الأمني بين العاملين، مما يساهم في بناء بيئة عمل أكثر أمانًا. إن الاستثمار في تكنولوجيا المعلومات وتطوير استراتيجيات فعالة لإدارة المخاطر سيكون له تأثير إيجابي على قدرة القطاع التأميني على مواجهة التحديات المستقبلية. في الختام، تقدم هذه الدراسة رؤى قيمة تساهم في تعزيز الأمان السيبراني في قطاع التأمين، مما يعكس أهمية التعاون بين مختلف الإدارات وتبني منهجيات متكاملة في إدارة المخاطر.

## النتائج

- 1- بلغ متوسط تقييم إدارة استثمارات تكنولوجيا المعلومات 4.10، مما يشير إلى أن المشاركين يعتبرون الإدارة والتطوير جزءًا أساسيًا من الموازنة ويعكس الالتزام بتخصيص الموارد اللازمة.
- 2- متوسط تقييم استراتيجية تكنولوجيا المعلومات بلغ 3.86، مما يدل على وجود تقييم مستمر، ولكن المشاركين يرون أن هناك حاجة للتحسين في كيفية تنفيذ التقييمات بشكل دوري.
- 3- متوسط تقييم الدخول المصرح به بلغ 3.97، مما يدل على اهتمام كبير بالأمان وضمان عدم دخول غير المصرح لهم إلى برامج القطاع التأميني.
- 4- متوسط تقييم دورات التدريب كان 4.00، مما يدل على أهمية تدريب العاملين وتمكينهم من استخدام التقنيات الحديثة بكفاءة.

- 5- بلغ المتوسط العام للمحور الأول 4.03، مما يدل على مستوى إيجابي عام في تقييم المشاركين لإدارة استثمارات تكنولوجيا المعلومات في القطاع التأميني.
- 6- بلغ المتوسط العام لاستجابات عينة الدراسة 3.85، مما يشير إلى مستوى إيجابي في تقييم العمليات الإلكترونية وإدارة المخاطر.
- 7- متوسط تقييم صحة المعاملات والمسؤولية كان 4.12، مما يعكس مستوى عالٍ من الثقة في العمليات الإلكترونية.
- 8- حصلت الفقرة الخاصة بضبط معايير الأنشطة الإلكترونية على متوسط 4.58، مما يدل على التزام قوي بمعايير الجودة والتحكم.
- 9- متوسط تقييم تحسين خدمات التأمين الإلكترونية بلغ 3.44، مما يشير إلى حاجة واضحة لتحسين هذه الخدمات لإرضاء العملاء.
- 10- متوسط الإشراف على مخاطر تكنولوجيا المعلومات كان 3.64، مما يدل على أن الإدارة تتم بشكل كافٍ، ولكن ليس بشكل مثالي.
- 11- بلغ متوسط إدارة التهديدات الإلكترونية 4.07، مما يعكس التزام القطاع بحماية المعلومات والبيانات من المخاطر.
- 12- متوسط التوسع في تقديم الخدمات كان 3.54، مما يدل على رغبة في التوسع، ولكن هناك حاجة لمزيد من الجهود في هذا الاتجاه.
- 13- متوسط حماية المعلومات وخصوصيتها بلغ 3.93، مما يشير إلى جهود القطاع في الحفاظ على خصوصية البيانات.
- 14- متوسط تعزيز الحماية من المخاطر الإلكترونية كان 3.53، مما يدل على وجود جهود، ولكن لا تزال هناك حاجة لتحسين هذه الجهود.
- 15- تشير النتائج إلى أن القطاع التأميني يبذل جهودًا ملحوظة في تأكيد صحة المعاملات وضبط المعايير، ولكن هناك حاجة واضحة لتحسين خدمات التأمين الإلكترونية وإدارة المخاطر.
- 16- بلغ المتوسط العام لاستجابات عينة الدراسة 3.74، مما يشير إلى تقييم إيجابي لأداء العاملين وعلاقتهم بالبرامج التدريبية.
- 17- متوسط تقييم المخاطر السيبرانية دوريًا كان 3.93، مما يدل على التزام القطاع بالتقييم المستمر للمخاطر.
- 18- حصلت الفقرة المتعلقة بالحد من مخاطر تكنولوجيا المعلومات على متوسط 3.53، مما يعكس فعالية إدارة المخاطر في الحد من المخاطر السيبرانية.
- 19- بلغ متوسط تحسين أداء المخاطر 3.74، مما يشير إلى وجود حاجة لتحسين الأداء عبر التأمين على بنية المعلومات.
- 20- متوسط تعزيز الأمان للمعلومات كان 3.90، مما يعني أن المشاركين يرون أن إدارة المخاطر تعزز الأمان، ولكن هناك حاجة لمزيد من الجهود.
- 21- حصلت فقرة تطوير نظم الحماية على متوسط 3.94، مما يعكس فعالية إدارة المخاطر في تطوير نظم الحماية.

- 22- بلغ متوسط الاعتماد على مصادر مرخصة 4.12، مما يدل على أهمية تحسين الاعتماد على أدوات الأمان الموثوقة.
- 23- متوسط إجراء اختبارات دورية بلغ 4.58، مما يشير إلى جهود جيدة في التحقق من استيفاء التطبيقات للمتطلبات الأمنية.
- 24- متوسط وجود قسم مخصص لإدارة المخاطر كان 3.44، مما يدل على ضعف الهيكل التنظيمي لدعم إدارة المخاطر.
- 25- بلغ متوسط المرونة اللازمة لحماية البيانات 3.64، مما يشير إلى الحاجة للتكيف مع التغيرات السريعة في بيئة التهديدات.
- 26- متوسط تحديث نظم الحماية كان 4.07، مما يعكس التزامًا بتحسين الأمان السيبراني بشكل مستمر.
- 27- بلغ متوسط تدريب العاملين على التصدي للمخاطر 3.54، مما يشير إلى أن إدارة المخاطر السيبرانية توفر تدريبًا مهمًا لتعزيز الوعي الأمني.
- 28- كان المتوسط العام لهذا المحور 3.74، مما يدل على مستوى إيجابي في تقييم المشاركين لإدارة المخاطر السيبرانية، مع وجود التزام قوي بالتطوير والتحسين.
- 29- تشير النتائج إلى أن إدارة المخاطر السيبرانية تعمل بشكل جيد على تقييم المخاطر وتطوير نظم الحماية، لكنها تحتاج إلى تحسين الأداء وتوفير هيكل تنظيمي قوي لدعم الإدارة.
- 30- تمت ملاحظة فروق في الاستجابات تعزى لمتغير الفئة الوظيفية عند مستوى دلالة 5%، حيث كانت الاستجابات إيجابية أكثر لدى العاملين في إدارة الأمن السيبراني ونظم المعلومات.
- 31- لم يكن لمتغير المؤهل العلمي تأثير معنوي على الاستجابات، حيث كانت قيمة اختبار Sig أكبر من مستوى الدلالة 5%.
- 32- أيضًا، لم يكن لمتغير عدد سنوات الخبرة تأثير معنوي على الاستجابات، حيث كانت قيمة اختبار Sig أكبر من مستوى الدلالة 5%.

## التوصيات

- 1- ينبغي على القطاع التأميني تطوير برامج تدريبية شاملة لتعزيز وعي العاملين بالأمن السيبراني، مما يساعد في تحسين قدرتهم على التصدي للمخاطر.
- 2- يجب التركيز على تحسين أداء إدارة المخاطر السيبرانية من خلال تطوير استراتيجيات فعالة تضمن استجابة سريعة وفعالة للتهديدات.
- 3- من الضروري تعزيز الهيكل التنظيمي لدعم إدارة المخاطر، مما يسهل اتخاذ القرارات السريعة في مواجهة التهديدات السيبرانية.
- 4- ينبغي أن يتم تحديث نظم الحماية بشكل دوري لضمان التكيف مع التغيرات المستمرة في بيئة التهديدات.
- 5- يجب تنفيذ تقييمات دورية للمخاطر السيبرانية لضمان تحديد التهديدات في وقت مبكر وتحسين استراتيجيات الحماية.
- 6- ينبغي تعزيز التعاون بين إدارات الأمن السيبراني والإدارات الأخرى لضمان تنفيذ استراتيجيات متكاملة وفعالة في إدارة المخاطر.

- 7- يجب تقييم أدوات الأمان المستخدمة بشكل دوري لضمان الاعتماد على مصادر مرخصة وموثوقة.
- 8- ينبغي زيادة الاستثمار في تكنولوجيا المعلومات لتعزيز البنية التحتية الأمنية وتطبيق أحدث التقنيات في مجال الأمن السيبراني.
- 9- يجب العمل على تحسين خدمات التأمين الإلكتروني لتلبية احتياجات العملاء وتعزيز ثقتهم في القطاع.
- 10- من الضروري رفع مستوى الوعي حول أهمية الأمن السيبراني بين جميع العاملين في القطاع، مما يساهم في خلق بيئة عمل أكثر أماناً.

#### المراجع:

- (1) إسماعيل، محمد، (2021)، التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن "المجلة الدولية للقانون، جامعة قطر.
- (2) زيد، أيمن، العمودي، (2015)، إدارة المخاطر في شركات التأمين دراسة قياسية بالتطبيق على الشركات الجزائرية للتأمين، مجلة رؤى اقتصادية والتجارية وعلوم التسيير، العدد9.
- (3) الكرعاي، زهراء، (2024)، دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين، مجلة الغري للعلوم الاقتصادية والإدارية، كلية الإدارة، مجلد 20.
- (4) مروة، القصاص، (2017)، دور نظم المعلومات الإلكترونية في إدارة مخاطر الصناعة التأمينية دراسة حالة عينة من شركات التأمين الجزائرية"، قسم العلوم الاقتصادية والقانونية، العدد 18.
- (5) إسماعيل، محمد (٢٠٢١م)، " التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة - دراسة في القانون القطري والمقارن "المجلة الدولية للقانون، المجلد العاشر، العدد الثالث عدد خاص بمؤتمر " القانون في مواجهة الأزمات العالمية - الوسائل والتحديات "، كلية القانون، جامعة قطر، ص ٢٠٦.
- (6) البردوني، ناريمان إسماعيل أحمد، (٢٠٢٥م)، " دور حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني وأثره في تحسين الأداء المالي: دراسة تجريبية على البنوك المقيدة بالبورصة المصرية"، مجلة الاسكندرية للبحوث، المحاسبية، كلية الأعمال، جامعة الإسكندرية، المجلد التاسع، العدد الأول، ص ١-٧١
- (7) الخياط، أحمد مصبح، (٢٠٢٠م)، " تصور مقترح لتطوير ادارة الأعمال في ضوء مدخل إدارة المخاطر بمؤسسات الأعمال الكويتية"، المجلة العلمية للاقتصاد والتجارة، كلية التجارة عين شمس ص٢٨.
- (8) الربيعية، صالح بن علي، (٢٠١٨م)، " الأمن الرقمي وحماية المستخدم من مخاطر الانترنت"، هيئة الاتصالات وتقنية المعلومات المملكة العربية السعودية.
- (9) الربيعي، خلود هادي وآخرون، (٢٠١٧م)، " أمن وسرية المعلومات وأثرها على الأداء التنافسي: دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية"، مجلة دراسات محاسبية ومالية، المعهد العالي للدراسات المحاسبية والمالية، جامعة بغداد المجلد، العدد ٢٣، ص٢٨٩-٣١٧.

- 10) الرحماوي، رحاب حسني، (٢٠٢٤م)، " إدارة المخاطر السيبرانية في المجال الاقتصادي"، مجلة الأمن القومي والاستراتيجية، الأكاديمية العسكرية للدراسات العليا والاستراتيجية، المجلد ٢، العدد ٤ ص ١٠٤-١١٥
- 11) السمحان، منى عبد الله صالح، (٢٠٢٠م)، " متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإلكترونية بجامعة الملك سعود " مجلة كلية التربية كلية التربية المنصورة، العدد ١١١، الجزء الأول، ص ٢٩٢
- 12) السميوي، سامي سعد (٢٠٢٢م)، " واقع الأمن السيبراني وتحدياته في السعودية"، المجلة العلمية الجامعة الملك فيصل: العلوم الأساسية والتطبيقية، المملكة العربية السعودية، المجلد ٢٣، العدد 1، ص ٦٦-٧٤
- 13) الطيب، أسامة محمد، (٢٠١٧م)، "إمكانية تطبيق تأمين الاخطار السيبرانية لحماية الفضاء السيبراني في جمهورية مصر العربية"، رسالة ماجستير، كلية التجارة، جامعة سوهاج، مصر.
- 14) العربي، أحمد عبادة، (٢٠١٥م)، " معيار المنظمة الدولية للتوحيد القياسي (ISO/IEC27002) لسياسات أمن المعلومات دراسة وصفية تحليلية لمواقع الجامعات العربية"، مجلة جامعة طيبة للآداب والعلوم الإنسانية كلية الآداب والعلوم الإنسانية، جامعة طيبة، السنة ٤، العدد ٧، ص ٧١١.
- 15) الكرعوي، زهراء مسافر عبيد، (٢٠٢٤م)، " دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين"، مجلة الغري للعلوم الاقتصادية والإدارية كلية الإدارة والإقتصاد، جامعة الكوفة، العراق، مجلد ٢٠، عدد ٢، ص ٤٥٦-٤٧٩.
- 16) المنصور، كاسر نصر، (٢٠٢٢م)، " إدارة المخاطر واستراتيجية التأمين في ظل تكنولوجيا المعلومات" الناشر: جامع الكتب الإسلامية المكتبة الشاملة الذهبية، ص ١٩.
- 17) آلدوي علي (٢٠٢٣م)، " الأمن السيبراني: تعريفه - أهميته - أنواعه - استراتيجيات الوقاية من الهجمات السيبرانية"، مجلة الدراسات الدولية، معهد الأمير سعود الفيصل للدراسات الدبلوماسية، وزارة الخارجية، العدد ٣٤، ص ١١٥-١٢٤.
- 18) النجار، عمر، (٢٠٢٠م)، " أثر إدارة المخاطر على التميز المؤسسي لجامعة الأقصى بقطاع غزة"، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية الجامعة الإسلامية غزة، فلسطين، ص ٢٨.
- 19) جرادات، ناصر محمد وآخرون، (٢٠١٩م)، " أثر الأمن المعلوماتي على أداء شركات التأمين العاملة في فلسطين"، المجلة المصرية للدراسات التجارية، جامعة المنصورة، كلية التجارة، المجلد ٤٣، العدد 4، ص ٢٠٠-٢٣٣.
- 20) جعفر، آل الشيخ، (٢٠٢٤م)، " أثر التحول الرقمي على إدارة مخاطر التأمين باستخدام تحليل السيناريوهات واختبار الإجهاد"، المجلة العربية للنشر العلمي، الإصدار السابع، العدد ٧١.
- 21) جمال الدين هبة، (٢٠٢٤م)، " الأمن السيبراني والتحول في النظام الدولي"، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد ٢٤، العدد ١، ص ٢٣٠-١٨٩.

<https://www.itu.int/net/ltunews/issues/2010/9/Pdf/201009-20-ar.pdf>."

22) 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.
- 23) Basel Committee on Banking Supervision, (2020), "Operational and cyber risks in the financial sector" - BIS Working Papers No 840, Bank for International Settlements.p6.
  - 24) Caliyurt, Kiymet. (2018)," Cyber security assurance process from the internal audit perspective". Managerial Auditing Journal Vol. 33 No. 4, pp. 360-376. <http://dx.doi.org/10.1108/MAJ-02-2018-1804>
  - 25) Eling, Martin, (2016)," Ten Kev Questions on Cyber Risk and Cyber Risk Insurance", The Geneva Association- International Association for the Study of Insurance Economics Zurich, Switzerland, p10.
  - 26) Foglietta, C., Masucci, D., Palazzo, C., Santini, R., Panzieri, S., Rosa, L., Cruz, T. and Lev, L. (2018), "From detecting evber-attacks to mitigating risk within a hybrid environment", IEEE Systems Journal, Vol. 13 No. 1, pp. 424-435. Doi: 10.1109/JSYST.2018.2824252
  - 27) Mott, S. Turner, J.R.C. Nurse et al, (2023), "Between a rock and a hard (ening) place: Cyber insurance in the ransomware era", Computers & Security, Vol. 128, May, 2023, pp. 103-162. <https://doi.org/10.1016/j.cose.2023.103162>
  - 28) 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. Doi: 10.1016/j.jfineco.2019.05.019
  - 29) Kuldeep Singh Kaswan et al. (2022), "Cybersecurity Law-based Insurance Market",ISBN: 978-1-80262-606-3, eISBN: 978-1-80262-605-6, Publication, July, 2022, pp.303-321. <http://doi.org/10.1108/978-1-80262-605-620221018>
  - 30) Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C. ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current & future trends. Information, 13(3), p146.