قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية

د. مصطفى زكي حسين متولي
مدرس بقسم المحاسبة والمراجعة
كلية التجارة – جامعة قناة السويس

د. حسين عبد العال سالم غريب
مدرس بالمعهد العالي للتسويق
والتجارة ونظم المعلومات – التجمع الأول

ملخص البحث:

استهدف البحث قياس أثر الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة في الشركات المصرية، من خلال توضيح مخاطر هجمات الأمن السيبراني وأهمية الإفصاح عنها، وتوضيح وتفسير العوامل المؤثرة في العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب المراجعة، حيث تمثل مجتمع الدراسة في الشركات المقيدة في البورصة المصرية والمتاحة للتحميل على الموقع الإلكتروني للبورصة المصرية، وتمثلت عينة الدراسة في عدد من هذه الشركات والتي يتوافر فيها بيانات قياس المتغيرات وعددها (١٥) شركة ، حيث تم الاعتماد على القوائم المالية للشركات عينة الدراسة خلال الفترة من ٢٠١٧ حتى ٢٠٢١، وتقارير الحوكمة، وتقرير هيكل المساهمين وهيكل مجلس الإدارة ومحاضر اجتماعات لجان المراجعة ومحاضر اجتماع الجمعية العمومية. وتوصلت نتائج الدراسة النظرية والتطبيقية إلى العديد من النتائج تمثل أهمها في وجود ارتباط إيجابي بين أتعاب عملية المراجعة ومخاطر اختراقات الأمن السيبراني، حيث أن مراجعي الحسابات عندما يجدون مخاطر الأمن السيبراني متزايدة يبذلون المزيد من الجهد أثناء عملية المراجعة الأمر الذى يؤدى إلى فرض أتعاب مرتفعة.

الكلمات الافتتاحية :الإفصاح عن مخاطر الأمن السيبراني، أتعاب المراجعة ، الهجمات السيبرانية .

Abstract:

The research aimed to measure the impact of Cyber security risks disclosure on Audit Fees in Egyptian companies. By clarifying the importance of Cyber security risks disclosure attacks, and explaining the factors affecting the relationship between disclosure of cyber security risks and audit fees, Where the study society is represented in the companies listed on the Egyptian Stock Exchange and available on its website, the study sample was represented in a number of these companies in which data measuring variables are available, where the financial statements of the study sample companies were relied on during the period from 2017 until 2021, governance reports, shareholder structure report, board of directors structure, audit committee meeting minutes and general assembly meeting minutes.

The results of the theoretical and applied study reached many results, the most important of which are the presence of a positive correlation between audit fees and the risks of cyber security breaches.As the auditors when they find the cyber security risks increasing they put more effort during the audit process which leads to imposing high fees.

Key words: Cybersecurity risks disclosure, Audit fee, Cyber attacks.

أولاً: فكرة البحث

في مجتمع المعلومات العالمي الحالي وحيث تنتقل المعلومات عبر الفضاء السيبراني، فإن الإدارة الفعالة لتلك المعلومات أمر بالغ الأهمية، وترتبط هذه الفعالية بالوعي بتزايد نقاط الضعف، مثل التهديدات السيبرانية وحرب المعلومات، فوفقاً لدراسة شركة IBM لعام ٢٠١٦، فإن تكلفة اختراق البيانات تصل إلى ٤ مليون دولار في المتوسط على مستوى العالم، بزيادة بنسبة ٢٩٪ في التكلفة الإجمالية منذ عام ٢٠١٣، وسجلت الولايات المتحدة أعلى متوسط تكلفة للفرد لإختراق البيانات عند ٢٢١ دولار في عام ٢٠١٦.Rosati, P, et al (2019)

فلقد أبدى مجلس الرقابة على شركات المحاسبة العامة PCAOB مخاوف بشأن المخاطر السيبرانية، وأوضح المجلس في خطته الاستراتيجية ٢٠٢٠-٢٠٢٤ أن أحد أهدافه هو: "تقييم بيئة أمن المعلومات المتغيرة وفهم المخاطر ذات الصلة، وبشكل أكثر تحديداً أوضح أن: "الوصول غير المصرح به إلى أنظمة المعلومات والبيانات يمكن أن يؤدي إلى التلاعب بالبيانات، وفقدان ملكية المعلومات، وتدمير الأنظمة، أو الإضرار بالسمعة. كما ينص المعهد الأمريكي للمحاسبين القانونيين المعتمدين(AICPA, 2018) على أن " الأمن السيبراني هو أحد أهم القضايا التي تشغل اهتمام الإدارات في كل الشركات في العالم كبيرة وصغيرة، عامة وخاصة" ، لذلك تكون الشركة مسئولة عن ماذا وكيف يتم الإفصاح عنه بشكل أكثر وضوحاً، ويركز (AICP,A2018) الضوء على أن الأمن السيبراني ليس مجرد مشكلة تقنية معلومات، ولكنه أيضاً مشكلة معنية بإدارة مخاطر المؤسسة والتي تتطلب حلاً عالمياً. وإدراكاً لذلك طالبت هيئة البورصة الأمريكية (SEC) بالإفصاح عن المخاطر المتعلقة بالأمن السيبراني، محذرة الشركات من تجنب الإفصاح عن عوامل الخطر التي يمكن أن تنطبق على أي مُصدر أو أي عرض.

كما وضع قانون Sarbanes-Oxley لعام ٢٠٠٢ (SOX) متطلبات صارمة على الشركات، تبرز أهمية ضوابط نظام المعلومات من خلال مطالبة الإدارة والمراجعين بالتقرير عن فعالية الرقابة الداخلية على عنصر التقارير المالية في نظم

معلومات إدارة الشركة، كما يتطلب SOX أن يكون لدى الشركات سياسات وإجراءات تمنع وتكشف عن مخاطر وحوادث الأمن السيبراني والتي يُحتمل أن تكون مهمة مادياً، ومن ثم فمن المحتمل أن يقوم المديرون بالإفصاح عن مخاطر الأمن السيبراني إذا كانوا يعتقدون أن احتمالية وقوع حادثة الأمن السيبراني في المستقبل عالية، وأن الآثار المحتملة للحادث كبيرة.

ولقد أكدت دراسة Masoud, N., & Al-Utaibi, G. (2022) على أهمية إعداد التقارير المالية لتقييم الآثار المترتبة على حوادث الأمن السيبراني، وبالتالي تتعلق أوجه القصور في إعداد التقارير المالية في المستقبل بمؤشرات مخاطر الأمن السيبراني، وعلى وجه الخصوص فإن الأسئلة المتعلقة بكيفية تأثير الإفصاح عن مخاطر الأمن السيبراني على تقييم الشركة بسبب التغيير في تصورات المخاطر تؤثر على أوجه القصور في التقارير المالية. فيما توصلت دراسة Benaroch, M., & Chernobai, A. (2017) أن الإفصاح عن مخاطر الأمن السيبراني والحوادث من قبل الشركات يفهم على أنه علامات على نقاط الضعف المادية للرقابة الداخلية في إعداد التقارير المالية، وبالتالي يمكن أن يمثل عوامل خطر كبيرة على جودة التقارير المالية الواردة في التقارير السنوية للشركات Lawrence, A., et al (2018) إضافة إلى ذلك يمكن أن تؤدي حوادث مخاطر الأمن السيبراني في المؤسسات الكبرى إلى إلحاق أضرار كبيرة بالشركات المخالفة من حيث تكاليف العلاج والغرامات والسمعة لسنوات (Rosati, P, et al (2019 .

وتظهر العديد من الدراسات التجريبية أن حوادث الأمن السيبراني عادةً ما تلحق الضرر بالأعمال التجارية والقيمة السوقية للشركات المتضررة (2020)؛ Kamiya, S., et al. ،Rosati, P., Gogolin, F., & Lynn, T. (2019) وتتعدد العوامل الأخرى التي وجد أنها تؤثر بشكل كبير على استجابة السوق لانتهاكات الأمن السيبراني والتي تتمثل في حجم الشركة ونوعها والصناعة ونصوص الإفصاح، وهذه العوامل تؤثر على عدد من أصحاب المصلحة الآخرين فإذا كانت إحدى الشركات تواجه مخاطر

مرتفعة في مجال الأمن السيبراني ولم يتم تنبيه المستثمرين بشأن هذه المخاطر وأصبحت في النهاية حادث أمن إلكتروني فعلياً فقد تتعرض الشركة لدعاوى قضائية.

وعلى الرغم من أن مضمون الأمن السيبراني يمتد عبر جميع مناطق الأعمال، إلا أن معظم اهتمام الأمن السيبراني في عالم الأعمال يركز على القطاع المالي لأنه وفقاً لدراسة Kamiya, S., et al. (2020) يؤدي هجوم المعلومات المالية إلى رد فعل سلبي في سوق الأسهم، وانخفاض في نمو المبيعات للشركات الكبيرة وشركات البيع بالتجزئة، وزيادة الرافعة المالية، وتدهور الصحة المالية، وانخفاض الاستثمار على المدى القصير. ومن ثم فلا شك إن اختراق أمن المعلومات المالية يمكن أن يؤدي بسهولة إلى انهيار شركة كبيرة في فترة زمنية قصيرة. ونتيجة لذلك في هذه السنوات الأخيرة، كان المنظمون وواضعو المعايير يبذلون مزيداً من القلق بشأن تهديدات الأمن السيبراني على مستوى اهتمام المراجعين الخارجيين، فلقد توصلت دراسة Rosati, P., et al (2019) إل أن الشركات التي تواجه اختراقاً يفرض عليها أتعاب مراجعة أعلى بنسبة ٢٨٪ مقارنة بالشركات غير المخترقة في عام حدوث اختراق في الأمن السيبراني للشركة، ويتم تفسير هذه الزيادة على أنها استجابة لزيادة مخاطر المراجعة وجهود المراجعة.

ولقد تناولت العديد من الدراسات العوامل المختلفة التي تؤثر على أتعاب المراجعة فقد أشارت دراسة Chu, J., et al (2018) أن عدم التأكد البيئي يعكس درجة المخاطر التي تواجهها الشركات والتي تحظى باهتمام خاص من قبل المراجعين في مرحلة تقييم المخاطر، حيث أنه كلما زاد عدم التأكد بشأن السياسة الاقتصادية، ارتفعت أتعاب المراجعة وبصفة الشركة لا يمكن أن تقاوم بشكل فعال ارتفاع مخاطر النظام في ظل حالة عدم تأكد بيئي كبيرة حتى لو حافظت على استمرار تحقيق أرباح عالية، ومن أجل تقليل مخاطر المراجعة يحتاج المراجعون إلى عمل إضافي لضمان جودة المراجعة ومنع الخسائر المتوقعة بعد ذلك سترتفع أتعاب المراجعة غير العادية،

بالإضافة إلى ذلك ستؤثر طبيعة حقوق ملكية الشركة أيضا على استمرار الأرباح وأتعاب المراجعة غير العادية.

كما أشار Hsieh, T. S., et al (2020) إلي أن أتعاب المراجعة تتأثر بشكل كبير بجهود المراجعين ومخاطر التقاضي والقدرة التفاوضية للمراجعين وعوامل أخرى، فالمراجعة هي خدمة مصادقة مستقلة، وتتقاضى مكاتب المحاسبة أتعابها ضمن النطاق الطبيعي وفقًا لتكاليف ومخاطر المراجعة، وفي بيئة تنافسية بالكامل يعكس التباين في أتعاب المراجعة بشكل أساسي الفرق بين تكلفة جهد المراجع والمخاطر المحددة للعميل، لذلك كلما زاد جهد المراجع زادت تكاليف المراجعة وكلما ارتفع التعويض، وبالمثل كلما زادت مخاطر العملاء زادت احتمالية فشل المراجعة وزادت احتمالية المقاضاة في المستقبل وزادت التكلفة المطلوبة للتعويض عن خسارة التقاضي في المستقبل، ومع ذلك فإن أتعاب المراجعة هي أيضاً نتيجة للمساومة بين أطراف المراجعة فإذا كانت أتعاب المراجعة أعلى بكثير من تكاليف المراجعة فمن المحتمل أن يكون لدى المراجعين اعتماد اقتصادي معين على الخاضعين للمراجعة.

حيث أصبح خطر حوادث اختراق البيانات أكثر تعقيداً وأكثر شيوعاً في بيئة الأعمال المترابطة اليوم، فقد أثارت الزيادة في حوادث اختراق البيانات حول العالم مخاوف بشأن كيفية حماية المؤسسات للمعلومات المسجلة الملكية والحفاظ على سلامة قواعد البيانات، ولذا فمن المتوقع أن يزيد المراجع الخارجي من الشك المهني فيما يتعلق بالحوادث الإلكترونية للشركات، فعلى الرغم من أن الشركات تعتقد أن هذه الحوادث لن تؤثر بشكل مباشر على البيانات المالية بطريقة مادية من الناحية الكمية، إلا أن وقوع حادث إلكتروني كبير سيحث المراجعين على بذل جهد كبير للتحقيق في الحادث وعادة بمشاركة المتخصصين، وذلك لأن خدمات المراجعين حول حادث إلكتروني تقع خارج نطاق المهام العادية للمراجعة، ولذا فإن ما تم تحديده مسبقا من أتعاب المراجعة فسيتم تعديلها لتعويض مراجع الحسابات عن الوقت والجهد المبذولين في التوصل إلى قرار بشأن تأثير الحادث السيبراني.

ثانياً: أهمية البحث

في ضوء ما تناولته فكرة البحث تتمثل الأهمية العلمية في وجود تضارب بين الدراسات والأدبيات المحاسبية حول العوامل المؤثرة على العلاقة بين إفصاح الشركات عن مخاطر الأمن السيبراني وأتعاب مراجع الحسابات، وبخاصة أن مراجعة مخاطر الأمن السيبراني تصنف في نطاق خدمات المراجعة الأخرى، كما تتمثل الأهمية العلمية في ندرة الدراسات المحاسبية التي تناولت تأثير مخاطر الأمن السيبراني على أتعاب مراجع الحسابات في البيئة المصرية.

وتتمثل أهميته العملية في اجتذاب الأمن السيبراني الكثير من الاهتمام في السنوات العشر الماضية، حيث تعتبر اختراقات الأمن السيبراني من أهم المخاطر التي تواجه الاقتصاد العالمي، فتعاني الشركات التي تتعرض لاختراق الأمن السيبراني من خسائر مالية وخسائر كبيرة في سمعتها، ونظراً للتأثير المحتمل على قيمة الشركة وعملياتها، أصبح الأمن السيبراني أحد أهم أولويات مجلس الإدارة والمديرين التنفيذيين، فيطالب المستثمرون بمزيد من المصداقية والشفافية في المعلومات حول مخاطر الأمن السيبراني واختراقات البيانات وكيفه تعامل الشركات مع هذه المخاطر، وبذلك يلعب جهد المراجع الخارجي دوراً محورياً وأساسياً في التأكيد على مثل هذه المهام وتوفير المزيد من المصداقية، الأمر الذى يؤدى إلى زيادة جهد عملية المراجعة بما ينعكس في ارتفاع أتعاب المراجع الخارجي.

ثالثاً: هدف البحث

يتمثل الهدف الرئيسي من البحث في قياس أثر الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجع الخارجي في الشركات المصرية، ويتحقق هذا الهدف من خلال توضيح مخاطر هجمات الأمن السيبراني وأهمية الإفصاح عنها، وتوضيح وتفسير العوامل المؤثرة في العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب المراجع الخارجي في الشركات المدرجة بالبورصة المصرية.

رابعاً: حدود البحث

لن يتعرض الباحثان بشيء من التفصيل للمتغيرات المتعددة التي قد تؤثر على أتعاب المراجع الخارجي والتي قد تتمثل في مخاطر التقاضي والقدرة التفاوضية للمراجع، كما لن يتعرض الباحثان لتأثير الإفصاح عن مخاطر الأمن السيبراني على الأبعاد المتعددة لعملية المراجعة والتي قد تتمثل في الإجراءات التحليلية وأدلة الاثبات وجودة عملية المراجعة، إضافة لذلك تم استبعاد المؤسسات المالية (البنوك، شركات التامين) من عينة البحث وذلك لما تتسم به تلك المؤسسات من خصائص تشغيلية تختلف اختلافاً جوهرياً عن الشركات الأخرى.

خامساً: خطة البحث

لتحقيق الهدف من البحث يتم تناوله من خلال أربع أقسام، حيث يتناول القسم الأول عرض وتحليل الأدبيات المحاسبية التي تناولت العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب المراجع الخارجي، فيما يتناول القسم الثاني الدراسة النظرية التي تشمل أهمية الإفصاح عن مخاطر الأمن السيبراني والعوامل المؤثرة على العلاقة بينه وبين أتعاب المراجع، ويتناول القسم الثالث الدراسة التطبيقية على الشركات المدرجة في البورصة المصرية، ويختتم البحث بالقسم الرابع من خلال عرض النتائج والتوصيات والدراسات المستقبلية.

القسم الأول: عرض وتحليل الأدبيات المحاسبية ذات الصلة

تقوم جميع الشركات بتخزين معلومات ذات قيمه كبيرة على شبكات المعلومات لكى تكون متاحة في أي وقت للمستخدمين، ونظراً لذلك فإن الأمن السيبراني يمثل مصدر قلق كبير لأعضاء مجلس الإدارة والمستثمرين غير المحترفين والمنظمين، وعلى الرغم من حقيقة أن عدد حوادث الأمن السيبراني وشدتها أخذت في الازدياد في الفترات الأخيرة، حيث وقعت حوادث معروفة جيداً في شركات كثيرة منها(Equifax Yahoo. Inc &Uber Technologies & Inc) إلا أنه يطلب من الشركات

الإفصاح عن معلومات قليلة نسبياً حول جهود إدارة مخاطر الأمن السيبراني وذلك استجابة لدعوات المستثمرين والمنظمين للحصول على المزيد من المعلومات، ولقد كانت تأثيرات هجمات الأمن السيبراني متعددة على أبعاد عملية المراجعة، ويختص الباحثان من هذه الأبعاد أتعاب المراجع الخارجي، حيث يتناول هذا القسم الأدبيات المحاسبية السابقة من خلال مجموعتين، تركز **المجموعة الأولى** على عواقب انتهاكات الأمن السيبراني والأحداث المتعلقة به محاسبياً، فيما **تركز المجموعة الثانية** على العلاقة بين مخاطر الأمن السيبراني وأتعاب عملية المراجعة، ويتم عرضهما على النحو التالي:

١-١ الدراسات التي تناولت الإفصاح عن مخاطر الأمن السيبراني

ركزت العديد من الدراسات الضوء علي الإفصاح عن الأمن السيبراني، فقد استهدفت دراسة Barry, T.,et al (2022) الاختلافات في الإفصاحات النوعية بين الشركات الصينية المدرجة في قوائم منفصلة بالولايات المتحدة ونظيراتها المحلية في الولايات المتحدة والتي تعكس الوعي بالأمن السيبراني على مستوى الشركة، وذلك توافقاً مع الإطار التنظيمي القوي في الصين الذي ينظم الأمن السيبراني، وتستكشف الدراسة أيضاً تأثير الإعداد المؤسسي على تقييم السوق للوعي بالأمن السيبراني من خلال دراسة حدث حول اعتقال المدير المالي لشركة Huawei، والتركيز على نقاط ضعف الأمن السيبراني في Huawei والتي من المحتمل أن تتحدى بشكل عام فعالية سياسات الأمن السيبراني الصينية، وقد توصلت الدراسة أنه بالنسبة لنظرائهم المحليين في الولايات المتحدة، فإن الشركات الصينية المدرجة في قوائم الشركات في الولايات المتحدة توفر قدراً أقل من الإفصاح عن الأمن السيبراني، ومع ذلك فإن تقييم السوق لإفصاحات الأمن السيبراني تكون أعلى بالنسبة للشركات الصينية المدرجة في البورصة، مما يشير إلى أن السوق ينظر بشكل أكثر إيجابية إلى إفصاحات الشركات الصينية التي تنقل مستوى أعلى من الوعي الداخلي بالأمن السيبراني، كما توفر

النتائج دليلاً على أن نظرة السوق للوعي بالأمن السيبراني للشركة حساسة للتغيرات في التصورات الخاصة بالإعداد المؤسسي للشركات.

وبحثت دراسة Masoud, N., & Al-Utaibi, G. (2022) في العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأوجه القصور في التقارير المالية، وتوصلت الدراسة إلي وجود تأثير تفاضلي بين عمليات الإفصاح عن مخاطر الأمن السيبراني في إعادة التقرير المالي قبل وبعد الاختراق المتعلق بحوادث الأمن السيبراني، يعتبر الارتباط بين الإفصاح عن مخاطر الأمن السيبراني وأوجه القصور المالية التي تم التقرير عنها لاحقاً إيجابياً وهاماً، حيث توفر الدراسة بعض الأدلة للمنظمين على أن المزيد من الإفصاح الخاص بالشركة قد يحقق جودة مراجعة أعلى، والتي يستجيب لها المراجع من خلال زيادة جهد المراجعة، وتشير النتائج التجريبية إلى أن الشركات التي لديها إفصاحات سابقة عن مخاطر الأمن السيبراني من المحتمل أن تواجه أوجه قصور في التقارير المالية.

كما وثقت دراسة Tosun, O. K. (2021) وجود ردود فعل سلبية كبيرة على أسعار الأسهم على المدى القصير لاختراق بيانات الشركات، وتحديداً فإن الشركات التي تتعرض لتسريب معلومات سرية تعاني من انخفاض كبير في العوائد اللاحقة مقارنة بالشركات التي لا يتم اختراقها، وقد يكون للإعلانات عن الاختراقات الأمنية مرتبطة سلباً بتغييرات أسعار الأسهم في خلال يومين من تاريخ الإعلان، فأوضحت الدراسة أنه في المتوسط يكون للإعلان عن اختراق أمن الشركات تأثير سلبي يبلغ حوالي ١٪ من القيمة السوقية للشركة في الأيام التي تلت الحدث، كما توصلت الدراسة إلى وجود اختلاف في تأثير هجمات الأمن السيبراني على أسعار الأسهم المتداولة ويرجع ذلك إلى اختلاف نوعية المعلومات التي يتم الحصول عليها من تلك الهجمات فإذا كانت هذه الهجمات تمثل اختراق للمعلومات الخاصة بالعملاء فسيفقد العملاء ثقتهم في الشركة ، ولكن إذا كانت الهجمات عبارة عن برامج خبيثة فإن التأثير المحتمل سيكون انخفاض التدفقات النقدية .

وحققت دراسة Kelton, A. S., & Pennington, R. R. (2020) في التأثير السلبي لانتهاكات الأمن السيبراني على شركة أخرى (غير مخترقة) في نفس الصناعة ، فيما يشار إليه باسم تأثيرات عدوى الاستثمار، وما إذا كانت عمليات الإفصاح عن الأمن السيبراني تخفف من هذه التأثيرات، وباستخدام تجربة مع مستثمرين غير محترفين توصلت الدراسة إلى أن جزءاً من المستثمرين المشاركين يعتبرون الاختراق خبراً إيجابياً للشركة غير المخترقة، وهي ظاهرة تُعرف باسم تأثيرات المنافسة، وتوصلت الدراسة إلى أن إفصاحات الأمن السيبراني المقدمة قبل إعلان الاختراق تخفف من تأثيرات العدوى، بالإضافة إلي أن إفصاحات الأمن السيبراني المقدمة بعد إعلان الاختراق يمكن أن تقلل من حجم أثار عدوى الاستثمار.

واستهدفت دراسة Yang, L., et al (2020) بناء نموذج لفحص تصور المستثمرين غير المحترفين تجاه إعداد تقرير الأمن السيبراني الذى طوره المعهد الأمريكي للمحاسبين القانونين المعتمدين، واعتمدت الدراسة التطبيقية في اختبار الفرضيات المقترحة على نمذجة المعادلة الهيكلية مع البيانات التي تم تجميعها من منصة Amazon's Mechanical Turk، وتوصلت نتائج الدراسة إلى أن الفوائد المتصورة للمستثمرين لإطار عمل مخاطر الأمن السيبراني مرتبطة بشكل إيجابي بنيّة الاستثمار، كما تؤثر جودة المعلومات والوعي بالأمن السيبراني أيضًا بشكل إيجابي على الفوائد المتصورة لإطار المخاطر ونية الاستثمار.

وقدمت دراسة Frank, M. L., et al (2019) دليلاً على فعالية التقارير الطوعية لإدارة مخاطر الأمن السيبراني والتأكيد المستقل، من حيث تعزيز جاذبية الاستثمار والتي تعتمد على ما إذا كانت الشركة قد أفصحت عن هجوم إلكتروني سابق. وافترضت الدراسة أن إصدار الإدارة لإطار عمل إعداد تقارير الأمن السيبراني الخاص بـ AICPA يكون أكثر فعالية عندما لا تفصح الشركة عن هجوم إلكتروني سابق، حيث يكون من غير المحتمل أن يشكك المستثمرين غير المحترفين في موثوقية تقارير الإدارة، ومع ذلك فإن الحصول على تأكيد من طرف ثالث لتقرير

الإدارة يوفر فائدة أكبر للشركات التي (لم تفصح) عن هجوم إلكتروني سابق، حيث تستفيد هذه الشركات أكثر من تعزيز موثوقية التأكيد، وتوصلت الدراسة إلى أنه قد يكون من الممكن تعزيز جاذبية استثمارات الشركة من خلال إصدار تقرير تأكيد مستقل بمفرده، وأن الأمن السيبراني يمثل مصدر قلق كبير للإدارة وأعضاء مجلس الإدارة والمستثمرين غير المحترفين والمنظمين.

وأفادت دراسة(Li, H., (2018 أن السوق يقدر بشكل إيجابي الوعي بالأمن السيبراني، ولذا فإن الشركات ذات النغمة السلبية في إفصاحات الأمن السيبراني لديها قيم سوقية أقل، ولهذا فإن الإفصاح عن عوامل الخطر هذه مرتبط بالحوادث السيبرانية التي يتم التقرير عنها في المستقبل، لما لها من قدرة على مساعدة أصحاب المصلحة في تقييم إمكانية حدوث أحداث سلبية في المستقبل (مثل حوادث خرق الأمن السيبراني)، وتوصلت الدراسة أن المعلومات التي يتم نقلها من خلال عمليات الإفصاح عن مخاطر الأمن السيبراني أمراً مهماً لأنه يساعد المستثمرين في تقييم مخاطر الأمن السيبراني للشركة وتزويد المنظمين بمعلومات حول ما إذا كانت القواعد التشريعية الإضافية ضرورية لتشجيع الشركات على الإفصاح أكثر عن مخاطر الأمن السيبراني الخاصة بهم.

١-٢ الدراسات التي تناولت العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب عملية المراجعة

تناولت العديد من الدراسات المحاسبية العوامل المؤثرة على أتعاب المراجعة، فيما تناولت دراسات أخرى الآثار المترتبة على أحداث الاختراق الإلكتروني الفعلية، بحجة أن الانتهاكات السيبرانية ستؤدى إلي زيادة خطر التحريف المادي وضعف الرقابة الداخلية وزيادة جهد المراجع والتأثير على جودة عملية المراجعة الأمر الذى يؤثر علي أتعاب مراجع الحسابات، ويمكن عرض هذه الدراسات من خلال الآتي:

ركزت دراسة Lim, Y., & Monroe, G. S. (2022) على اختبار العلاقة بين تغطية المحللين وأتعاب المراجعة، واختبار ما إذا كان تبنى المعايير الدولية لإعداد التقارير المالية (IFRS) وحماية المساهمين على مستوى الدولة يتفاعل مع تغطية المحللين للتأثير على أتعاب المراجعة، وتعزز هذه الدراسة فهم تأثير تغطية المحللين على أتعاب المراجعة فيما يتعلق باعتماد المعايير الدولية لإعداد التقارير المالية ومستويات حماية المساهمين في بيئة دولية، وباستخدام ٤١٦٤٨ ملاحظة لعدد ٣٠ دولة خلال الفترة من ٢٠٠٠ حتى ٢٠١١ توصلت الدراسة إلى أن المراجعين يفرضون أتعاب مراجعة أعلى عندما يكون لدى الشركات تغطية أكبر للمحللين، كما توصلت الدراسة إلى أن التأثير الإيجابي لتغطية المحللين على أتعاب المراجعين أضعف بالنسبة للشركات التي تعتمد المعايير الدولية لإعداد التقارير المالية في الدول التي توجد فيها حماية عالية للمساهمين.

فيما هدفت دراسة Hansen, J. C., et al (2022) إلي قياس تأثير المخاطر القانونية على مستوى الولاية على تسعير أتعاب المراجعة في الولايات المتحدة الأمريكية، حيث تفترض هذه الدراسة أن المراجعين أكثر عرضة لفرض أتعاب مراجعة أعلى على العملاء الذين يقع مقرهم الرئيسي في دول ذات مخاطر قانونية أعلى من حيث احتمال رفع دعوى قضائية ، والحجم المتوقع للأضرار المخصصة لمراجعي الحسابات، واتساع نطاق الأطراف القادرة على المطالبة بالتعويضات، حيث تفترض هذه الدراسة أن المخاطر القانونية المرتفعة على مستوى الدولة تؤدي إلى أتعاب مراجعة أعلى، ولاختبار ذلك تقدر هذه الدراسة انحدارات المربعات الصغرى العادية لأتعاب المراجعة لـعدد ٥٦،٥٧٦ شركة في الفترة من ٢٠٠١ حتي ٢٠١٨ ، وتوصلت الدراسة إلي أن المخاطر القانونية على مستوى الولاية مرتبطة بشكل إيجابي بتسعير أتعاب المراجعة .

واستهدفت دراسةChi, W.,et al. (2022) اختبار العلاقة بين عملية إعادة إصدار القوائم المالية وزيادة أتعاب المراجعة، وباستخدام مجموعة من بيانات الشركات في

الولايات المتحدة وتايوان، وتوصلت الدراسة إلى أن انخفاض أتعاب المراجعة بين الشركات غير المعاد صياغتها والتي ارتبط شريكها في عملية المراجعة مؤخراً بإعادة صياغة عميل آخر، حيث أشارت الدراسة إلى أن هذه النتائج تكون أقوى بشكل عام عندما تكون إعادة الصياغة المرتبطة بالشريك أكثر وضوحًا أو شدة ، وفي الولايات المتحدة عندما يكون العملاء غير المعاد صياغتهم في نفس الصناعة العميل المعاد صياغته. على الرغم من أن الدراسة توصلت إلى أدلة محدودة للغاية على أن ضغوط الأتعاب تؤدي إلى عمليات مراجعة منخفضة الجودة للعملاء الآخرين لهؤلاء الشركاء في تايوان ، وجدنا أنه عندما تكون إعادة الصياغة المرتبطة بالشريك أكثر بروزًا أو شدة ، فإن ضغوط الأتعاب تؤثر سلباً على جودة المراجعة في الولايات المتحدة.

وهدفت دراسة Zhang, Y., & Smith, T. J.(2022) إلى قياس تأثير اختراقات شركات العملاء للبيانات على أتعاب مراجعة مورديها ضمن علاقة سلسلة التوريد الخاصة بشركات العملاء والشركات الموردة، حيث فحصت الدراسة ما إذا كانت حوادث اختراق البيانات لشركات العملاء مرتبطة بشكل إيجابي بأتعاب المراجعة الخاصة بمورديها، وتوصلت الدراسة إلى وجود ارتباطاً إيجابياً بين الإفصاح عن انتهاكات شركة العميل وأتعاب المراجعة الخاصة بالمورد حيث أن هذا الارتباط موجود لكل من اختراقات البيانات الداخلية والخارجية. كما توصلت الدراسة أيضاً إلى أن هذا الارتباط يختلف بشكل متوقع بناءً على قوة علاقة سلسلة التوريد الأساسية، وأن أتعاب المراجعة تكون أعلى عندما يكشف المزيد من العملاء عن انتهاكات في سلسلة التوريد في سنة معينة.

بينما تناولت دراسة Pacheco, A., & Wheatley, C. M.(2022) ما إذا كان مراجعي الحسابات يعدلون تقييماتهم لمخاطر الأعمال عندما تشتري الشركات محل المراجعة منتجات التأمين الإلكتروني، وكان التساؤل الرئيسي في الدراسة هل توجد علاقة ارتباط بين التأمين الإلكتروني وأتعاب المراجعة، وقد توصلت الدراسة إلى أن الشركات التي لديها تأمين إلكتروني بشكل عام تعتبر ذات مخاطر أعلى من الشركات التي ليس لديها تأمين إلكتروني، وبررت الدراسة هذه النتيجة بأن شراء التأمين

الإلكتروني يدل على ملف مخاطر أعلى بشكل عام ويؤدى هذا إلى زيادة أتعاب عملية المراجعة، كما توصلت الدراسة إلى أن إسناد الإشراف على الأمن السيبراني إلى لجان المراجعة مرتبط بإدراك المراجع لوجود مخاطر أقل .

وتناولت دراسة Rosati, P., et al (2022) تقيم أثر جودة المراجعة على اختراق البيانات لعينة كبيرة من الشركات الأمريكية، وبالاعتماد على منهج الاختلاف في الفروق المستند إلى عينة مطابقة من الشركات المخترقة والشركات التي لم يتم اختراقها توصلت الدراسة إلى عدم وجود أدلة على أن حوادث الأمن السيبراني تؤدى إلى انخفاض جودة المراجعة، كما استنتجت الدراسة أن الشركات المخترقة تشهد انخفاضاً في الاستحقاقات غير الطبيعية، وتكون أقل احتمالا للإفصاح عن الأرباح المنخفضة أو الزيادة المنخفضة في الأرباح، ومن المحتمل أن يتم إصدار تقرير الاستمرارية، بينما من غير المحتمل إعادة إصدار القوائم المالية في العامين التاليين لعملية الاختراق، كما تشير النتائج إلى أن المراجعين عوضوا بشكل فعال الزيادات في مخاطر المراجعة من خلال الاختبارات الجوهرية وجهد المراجعة بما يدعم وجهه النظر بأن مراجعي الحسابات زادوا من وعيهم بمخاطر المراجعة ووضعوا إجراءات مناسبة للتعامل مع عواقب حوادث الأمن السيبراني.

واستهدفت دراسة Perols, R. R., & Murthy, U. S. (2021) تأثير التأكيد المشترك أو المنفصل لبرامج إدارة مخاطر الأمن السيبراني على تصورات المستثمرين وقراراتهم، وما إذا كانت هذه التأثيرات تختلف عند وقوع حادث أمن إلكتروني لاحق، وذلك استجابة لمخاطر الأمن السيبراني والطلب على معلومات حول برامج إدارة مخاطر الأمن السيبراني للمؤسسات، ووفقاً لما أصدر عن المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) مؤخراً لخدمة فحص مخاطر الأمن السيبراني بحثت الدراسة في الخدمات الناشئة غير المتعلقة بالمراجعة وكيف يمكن لإشارة جودة الخدمات الأخرى بخلاف المراجعة أن تؤثر على تصورات جودة المراجعة، وتوصلت إلى أن الإشارة السلبية لحادث أمن إلكتروني لاحق يعكس

تصورات المستثمرين الإيجابية لكفاءة مراجع الحسابات ويزيد من حساسية المستثمرين لإعاقات الاستقلال المحتملة عندما يتم توفير الأمن السيبراني بشكل مشترك، مما يؤدي إلى تصورات أقل لجودة مراجعة منخفضة، كما توصلت الدراسة إلى أنه يتم تصنيف اختبارات الأمن السيبراني على أنها خدمات غير مسموح بها للمراجعة ويمكن للمنظمات الحصول على فحص للأمن السيبراني من نفس مراجع القوائم المالية، أو من مراجع منفصل.

فيما ذكرت دراسة Bao Ngo, T. N., & Tick, A. (2021) أن ارتفاع هجمات الأمن السيبراني قد أثار الكثير من المخاوف بشأن تكاليف هذه الهجمات وتأثيراتها المحاسبية على الشركات، الأمر الذى دعي إلى التساؤل عن مدى استجابة مراجعي الحسابات لهذه الهجمات، وتمثل الهدف الرئيسي من الدراسة في البحث عن ما إذا كان مراجعي الحسابات يركزون بشكل أكبر على الشركات التي تتعرض لهجمات الأمن السيبراني من خلال فرض أتعاب مراجعة أعلى، واعتمدت منهجية الدراسة على عينة مكونة من ١٠٠ شركة عالمية صغيرة ومتوسطة وكبيرة الحجم، وتوصلت الدراسة إلى وجود ارتباط إيجابيي بين أتعاب عملية المراجعة واختراقات الأمن السيبراني، وتتفق هذه النتيجة مع العديد من الدراسات في أن مراجعي الحسابات عندما يجدون المزيد من مخاطر الأمن السيبراني يبذلون المزيد من الجهد أثناء عملية المراجعة الأمر الذى يؤدى إلى فرض أتعاب مرتفعة.

بينما بحثت دراسة Li, H., Huang, F., Sun, Z., & Wang, T. D.(2020) فيما إذا كانت خبرة المراجع الخارجي مع حوادث الأمن السيبراني لعملائهم تؤثر على جهود المراجعة اللاحقة مع العملاء غير المخترقين وتساعد هؤلاء العملاء على تقليل مخاطر الأمن السيبراني. وذكرت الدراسة أن مكاتب المراجعة التي لديها خبرة مع العملاء المخترقين للأمن السيبراني مع افتراض ثبات باقي المتغيرات تفرض أتعاب مراجعة أعلى من العملاء غير المخترقين وهي ظاهرة موجودة فقط في مكاتب المراجعة الأربعة الكبار ومكاتب المراجعة مع الخبرة في

مجال تكنولوجيا المعلومات، وتوصلت الدراسة إلي أن زيادة أتعاب المراجعة مرتبطة سلباً بانتهاكات العملاء غير المخترقة في المستقبل، وأشارت النتائج أيضاً إلي أن مكاتب المراجعة يمكنها الاستفادة بنجاح من خبرة الأمن السيبراني في عمليات المراجعة، وهذا له آثار مهمة على مجلس مراقبة شركات المحاسبة العامة (PCAOB) فيما يتعلق بكيفية قيام المراجعين بتضمين مخاطر الأمن السيبراني أو على وجه التحديد انتهاكات الأمن السيبراني السابقة في تقييماتهم لمخاطر العملاء غير المخترقين.

وبحثت دراسة Li, H., No, W. G., & Boritz, J. E. (2020) في ثلاث نقاط جوهرية تتمثل في : مدى استجابة مراجع الحسابات للحوادث السيبرانية من خلال فرض أتعاب مراجعة أعلى، وما إذا كان مراجع الحسابات يتوقعون مخاطر الأمن السيبراني الجوهرية وتسعيرها قبل وقوع الحوادث السيبرانية، وما إذا كانت الزيادات في أتعاب المراجعة للشركات التي تواجه حادثًا إلكترونياً في الفترة الحالية مرتبطة بالحوادث الإلكترونية اللاحقة، وتوصلت الدراسة إلى أن الحوادث السيبرانية فقط هي التي ترتبط بزيادة أتعاب المراجعة وأن الارتباط مدفوع بحوادث أكثر خطورة، كما أن الزيادات في أتعاب المراجعة تكون أقل بالنسبة للشركات التي لديها إفصاح سابق عن مخاطر الأمن السيبراني بعد عام ٢٠١١ عندما أصدرت لجنة الأوراق المالية والبورصات إرشادات الإفصاح عن الأمن السيبراني، وأن الزيادات الأكبر في أتعاب المراجعة للشركات التي تواجه حوادث إلكترونية في الفترة الحالية ترتبط بانخفاض احتمالية وقوع حوادث إلكترونية لاحقة.

فيما تناولت دراسة Rosati, P., Gogolin, F., & Lynn, T. (2019) تأثير حوادث الأمن السيبراني على أتعاب المراجعة وباستخدام عينة مكونة من ٥٦٨٧ شركة، توصلت الدراسة إلى أن أتعاب المراجعة للشركات التي بها اختراق أمني شهدت زيادة بنسبة ١٢٪ في أتعاب المراجعة الخاصة بها ، وشهدت الشركات في نفس الصناعة التي تعرضت فيها الشركة المخالفة زيادة بنسبة ٥٪ في أتعاب المراجعة، كما

قدمت الدراسة دليل على أن مراجع الحسابات لا يراجعون تقييم مخاطر المراجعة بعد حدوث اختراق، وبشكل عام تشير هذه النتائج إلى أن الزيادة في أتعاب المراجعة في سنة الاختراق مؤقتة فقط، وأن مراجع الحسابات يدرجون مخاطر الأمن السيبراني في تقييمهم لمخاطر المراجعة حتى قبل وقوع أي حادث، وتنعكس مخاطر الأمن السيبراني المرتفعة في نهاية الأمر في شكل في ارتفاع أتعاب المراجعة.

واستهدفت دراسة Smith, T. J., et al (2019) قياس أثر انتهاكات أمن البيانات على عمليات الشركات، حيث ذكرت الدراسة أن مراجع الحسابات يعمل كآلية حوكمة خارجية مهمة فيما يتعلق ببروتوكول إدارة المخاطر الشامل للشركة، وبالتالي فحصت الدراسة ما إذا كانت مخاطر الاختراق قد تؤدى إلى زيادات محتملة في أتعاب المراجعة، وباستخدام عينة من الشركات التي تم اختراقها خلال الفترة من ٢٠٠٥ حتى ٢٠١٤ توصلت الدراسة إلى أن وجود لجان مخاطر على مستوى مجلس الإدارة ولجان مراجعة أكثر نشاطاً قد يساعد في التخفيف من علاوة أتعاب مراجعة مخاطر الاختراق ، كما تشير النتائج إلى أن كلاً من عمليات الإفصاح عن الاختراقات السابقة وكذلك الإفصاحات المستقبلية مرتبطة بأتعاب المراجعة.

وركزت دراسة Yen, J. C., et al (2018) على قياس تأثير خصائص شركات المراجعة على العلاقة بين أتعاب المراجعة وحوادث اختراق أمن المعلومات، واستخدمت الدراسة إدراك مخاطر أمن المعلومات كوكيل عن مستوى مخاطر أمن معلومات الشركة ، كما ذكرت الدراسة أنه لفحص جهود المراجعين لفهم وتقييم مخاطر وإجراءات أمن معلومات العملاء تستخدم أتعاب المراجعة المفروضة على العميل في الفترة اللاحقة للانتهاكات، ولتقديم أدلة تجريبية اعتمدت الدراسة على تجميع انتهاكات أمن المعلومات المفصح عنها من قاعدة DataLossDB خلال الفترة من ٢٠٠٤ حتى ٢٠١٣، وتوصلت الدراسة إلى وجود ارتباط إيجابي بين انتهاكات أمن المعلومات المفصح عنها وأتعاب المراجعة اللاحقة ، وأن خبرة الصناعة تخفض الارتباط بين انتهاكات أمن المعلومات وأتعاب المراجعة من ٥٢% إلى ١١,٣% ، كما أن فترة

المراجعة الطويلة تقلل الارتباط من ١٣,٧% إلى -١٢,٤% ، كما توصلت إلى أن خصائص شركات المراجعة تساعد المراجعين في تقييم مخاطر أمن المعلومات بشكل أفضل وتقييم عمليات إدارة أمن المعلومات بجهد أقل.

١-٣ تحليل الدراسات السابقة

في ضوء ما جاءت به الأدبيات المحاسبية ذات الصلة بمجال الإفصاح عن مخاطر الأمن السيبراني وأتعاب مراجع الحسابات فإن للباحثان أن يناقش أهم ما توصلت إليه هذه الدراسات من خلال النقاط التالية:

ركزت العديد من الدراسات وبشكل كبير على الإفصاح عن مخاطر الأمن السيبراني من خلال مناقشة أهم الهجمات الإلكترونية المتكررة وعواقبها والتي تمت خلال السنوات الأخيرة وبخاصة في دولتي الصين والولايات المتحدة على اعتبارهم من أكبر الدول التي تعرضت لهذه الهجمات، وفى ضوء اهتمام هذه الدراسات بالشق المحاسبي تناولت علاقة مخاطر الأمن السيبراني بالتقارير المالية قبل وبعد الهجمات الالكترونية، فتوصلت دراسة Masoud, N., & Al-Utaibi, G. (2022) إلى أن الشركات التي لديها إفصاحات سابقة عن مخاطر الأمن السيبراني من المحتمل أن تواجه أوجه قصور في التقارير المالية، فيما استهدفت دراسة Barry, T.,et al (2022) الاختلافات في الإفصاحات النوعية بين الشركات الصينية المدرجة في قوائم منفصلة بالولايات المتحدة ونظيراتها المحلية في الولايات المتحدة والتي تعكس الوعي بالأمن السيبراني على مستوى الشركة، وقدمت دراسة Frank, M. L., et al (2019)) دليلاً على فعالية التقارير الطوعية لإدارة مخاطر الأمن السيبراني والتأكيد المستقل ، من حيث تعزيز جاذبية الاستثمار والتي تعتمد على ما إذا كانت الشركة قد أفصحت عن هجوم إلكتروني سابق.

توصل الباحثان إلى وجود اتفاق بين بعض الدراسات على أن الإفصاح عن مخاطر الأمن السيبراني يعد من أهم العوامل المؤثرة على أتعاب عملية المراجعة،

حيث ذكرت العديد من الدراسات أن الحوادث السيبرانية ترتبط بزيادة أتعاب عملية المراجعة وأن هذا الارتباط مدفوع بالمخاطر الناتجة عن هذه الحوادث، إضافة إلى أن الزيادات في أتعاب المراجعة قد تكون أقل بالنسبة للشركات التي لديها إفصاح سابق عن مخاطر الأمن السيبراني.

فيما اختلفت العديد من الدراسات حول العوامل التي تؤثر على العلاقة بين مخاطر هجمات الأمن السيبراني وأتعاب المراجعة، فقد توصلت دراسة Zhang, Y., & Smith, T. J.(2022) إلى أن أتعاب المراجعة تكون أعلى عندما يكشف المزيد من العملاء عن انتهاكات في سلسلة التوريد في سنة معينة، فيما استنتجت دراسة Pacheco, A., & Wheatley, C. M.(2022) أن شراء التأمين الإلكتروني يدل على ملف مخاطر أعلى بشكل عام ويؤدى هذا إلى زيادة أتعاب عملية المراجعة. بينما توصلت دراسة Bao Ngo, T. N., & Tick, A. (2021) إلى وجود ارتباط إيجابيي بين أتعاب عملية المراجعة واختراقات الأمن السيبراني، حيث أن مراجع الحسابات عندما يجدون المزيد من مخاطر الأمن السيبراني يبذلون المزيد من الجهد أثناء عملية المراجعة الأمر الذى يؤدى إلى فرض أتعاب مرتفعة. فيما بحثت دراسة Li, H., Huang, F., Sun, Z., & Wang, T. D.2020. فيما إذا كانت خبرة المراجعين مع حوادث الأمن السيبراني لعملائهم تؤثر على جهود المراجعة اللاحقة مع العملاء غير المخترقين وتساعد هؤلاء العملاء على تقليل مخاطر الأمن السيبراني. كما توصلت دراسة Smith et al. (2019) إلى أن وجود لجان مخاطر على مستوى مجلس الإدارة ولجان مراجعة قد يساعد في التخفيف من علاوة أتعاب مراجعة مخاطر اختراقات الأمن السيبراني، وذكرت دراسة Yen, J. C., et al (2018) أن خصائص شركات المراجعة تؤثر على العلاقة بين أتعاب المراجعة وحوادث اختراق أمن المعلومات.

واستنتج الباحثان من خلال تحليلهما وجود اتفاق فيما بين الدراسات على أن الفوائد المدركة لإطار عمل مخاطر الأمن السيبراني تؤثر بشكل كبير على جودة

المعلومات والوعى بالأمن السيبراني ، وأن الإشارة لحوادث الأمن السيبراني اللاحقة لعملية المراجعة قد تؤثر بشكل كبير على تصورات المستثمرين المدركة بخصوص جودة عملية المراجعة الأمر الذى يعرض المراجع الخارجي لمخاطر التقاضي، ولذا زاد وعى المراجع بإجراء المزيد من الجهد عند إجراء عملية المرجعة وبخاصة في الشركات التي تعرضت لإختراقات الأمن السيبراني، فيما جاءت النتائج متضاربة بشأن العلاقة بين الإفصاح عند اختراقات الأمن السيبراني على أتعاب عملية المراجعة، ويعتقد الباحثان أن هناك علاقة إيجابية ومعنوية بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب عملية المراجعة وبخاصة في الشركات التي سبق وأن حدث بها عمليات اختراق، وفى حين لم تتناول أياً من الدراسات والأدبيات المحاسبية العلاقة بين الأمن السيبراني وأتعاب عملية المراجعة في البيئة المصرية فإن الباحثان يستهدفان من هذه الدراسة توضيح هذه العلاقة في البيئة المصرية.

القسم الثاني : الدراسة النظرية واشتقاق الفروض البحثية

٢-١ الأبعاد المتعددة لمخاطر الأمن السيبراني من منظور محاسبي

أدت حوادث الأمن السيبراني البارزة في الشركات العامة إلى زيادة حساسية المستثمرين لمثل هذه الحوادث وزيادة الطلب على المعلومات حول برامج إدارة مخاطر الأمن السيبراني للمؤسسات، فعرفت حوادث الأمن السيبراني (أو الاختراقات الأمنية) على أنها أي حدث يخل بسرية أصل المعلومات أو سلامته أو توفره، على هذا النحو قد تتكون حوادث الأمن السيبراني من أنواع مختلفة من الأحداث مثل البرامج الضارة، برامج الفدية، هجمات رفض الخدمة أو الاحتيال عند استخدام بطاقات الائتمان أو حتى الخطأ البشري، وغالباً ما يكون من الصعب اكتشاف حوادث الأمن السيبراني وتقدير تأثيرها المحتمل، فالسجلات المفقودة أو المسروقة والتكاليف المباشرة وغير المباشرة المرتبطة بها يجعل من اكتشاف مثل هذه الحوادث عملية معقدة (Perols, R. R., & Murthy, U. S. (2021 .

وغالباً ما يتم استخدام مصطلحات الأمن السيبراني وأمن المعلومات بالتبادل، حيث يصف المعهد الأمريكي للمحاسبين القانونين AICPA (2017) الأمن السيبراني بأنه عملية تنفيذ وتشغيل الضوابط وأنشطة إدارة المخاطر الأخرى لحماية المعلومات والأنظمة من الأحداث الأمنية التي يمكن أن تعرضها للخطر عندما لا يتم منع الأحداث الأمنية، لاكتشاف، الاستجابة، التخفيف، والتعافي من تلك الأحداث في الوقت المناسب، وتعرف اختراقات الأمن السيبراني على أنها فقدان السرية أو النزاهة أو توافر المعلومات، بما في ذلك أي إعاقة ناتجة عن (١) تكامل المعالجة أو توافر الأنظمة أو (٢) نزاهة أو توفر مدخلات أو مخرجات النظام، والتي لها تأثير سلبي على تحقيق أهداف والتزامات أعمال المؤسسة (بما في ذلك التزامات الأمن السيبراني) وكذلك القوانين واللوائح المتعلقة بمخاطر الأمن السيبراني وبرنامج الأمن السيبراني، حيث سيعاني الفضاء الإلكتروني من حدث أمني أو اختراق في وقت ما.

وقد أوضحت دراسة Hsu, C., et al. (2016) أن القضايا المتعلقة بإدارة مخاطر أمن المعلومات تشمل الاستثمار في أمن المعلومات، ومشاركة المعلومات الأمنية، وبرامج التوعية بأمان المستخدم، ودور فريق الإدارة العليا أو مجلس الإدارة، والعوامل المؤسسية المؤثرة على إدارة مخاطر أمن المعلومات، واعتماد معايير أمن المعلومات، وسياسة الأمن، وأنه غالباً ما يتم استخدام عبارة "حادث الأمن السيبراني" بشكل مشابه للإشارة إلى أمن المعلومات. وأشارت دراسة Rosati, P., et al. (2019a) إلي أن عدد حوادث الأمن السيبراني تتزايد كل عام خاصة بسبب الاستخدام المتزايد للإنترنت والحوسبة السحابية والأجهزة المحمولة، ويمكن أن تؤدي حوادث الأمن السيبراني إلى أضرار جسيمة للشركات التي تم اختراقها من حيث تكاليف المعالجة والغرامات والسمعة حيث تعتبر حوادث الأمن السيبراني أحداثاً معقدة ومتعددة الأوجه وقد لا تتحقق دائماً آثارها الكاملة على الفور.

وعرف Pacheco, A., & Wheatley, C. M. (2022) المخاطر الإلكترونية على أنها المخاطر المرتبطة بحدث إلكتروني خبيث يتسبب في تعطيل الأعمال

التجارية وخسائر مالية، واستجابة لذلك تهدف نظم إدارة المخاطر إلى تقييم المخاطر واتخاذ خطوات لتقليلها إلى مستوى مقبول، ويمكن تقسيم إدارة المخاطر إلى نشاطين أساسيين هما (تقييم المخاطر والتخفيف من حدة المخاطر) بالنسبة لتقييم المخاطر يحدد المديرون المخاطر بناءً على البنية التحتية للمؤسسة، وبمجرد تحديد التهديدات والمخاطر يمكن للمديرين تجاهل المخاطر أو تخفيفها أو نقلها أو الاحتفاظ بها، بينما يتضمن التخفيف من حدة المخاطر اختيار وتنفيذ الضوابط الأمنية لتخفيضها إلى مستوى مقبول للإدارة، وقد تقوم المنظمات أيضاً بتحويل المخاطر المالية عن طريق شراء تأمين متخصص، يوفر للمؤسسة الأمان ضد المخاطر وعدم التأكد، ويساعد في تقليل احتمالية الخسارة المالية.

٢-١-١ مدى تأثر القوائم المالية للشركات بمخاطر هجمات الأمن السيبراني

تزايدت قضايا الأمن السيبراني الكثير في السنوات الأخيرة خاصة بعد العديد من الهجمات الإلكترونية رفيعة المستوى، على شركات Sony & Equifax Inc Target Corporation &Pictures Entertainment Inc، حيث ارتفع متوسط عدد الحوادث الإلكترونية المكتشفة بنسبة ٣٨%، وأن سرقة الملكية الفكرية زادت بنسبة ٥٦% في عام ٢٠١٥ مقارنة بعام ٢٠١٤، وقد أبدى المنظمون وواضعو المعايير قلقهم بشأن تهديدات الأمن السيبراني في عدة سنوات، ولذا صرحت SEC أن تأثير الهجمات الإلكترونية قد يمتد إلى ما هو أبعد من التكاليف المباشرة المرتبطة بالرد الفوري على أي هجوم، وبالإضافة إلى الضرر غير المقبول للمستهلكين، تشمل هذه الآثار الثانوية الإضرار بالسمعة الذي يؤثر بشكل كبير على أرباح الشركة Li, H., et al. (2020).

ولهذا فإن القضايا المتعلقة بالأمن السيبراني حظيت باهتمام متزايد من قبل الأكاديميين والهيئات التنظيمية، حيث كلفت حوادث الأمن السيبراني الشركة الأمريكية في المتوسط حوالي ١٥,٤ مليون دولار سنوياً Griffiths, J. 2015 ، ومن المقدر أن تصل تكلفة الانتهاكات الإلكترونية العالمية إلى ٦ تريليونات دولار بحلول عام ٢٠٢٥، وينظر الرؤساء

التنفيذيون إلى الأمن السيبراني علي اعتباره أحد أكبر عشرة تهديدات للنمو المستقبلي، ويعبرون عن قلقهم بشكل متكرر بشأن التأثير السلبي لقضايا الأمن السيبراني على ثقة أصحاب المصلحة في شركتهم وفي الصناعة Héroux, & Gao, L., et al. (2020) S., &، كما تزايدت المخاطر والتهديدات المرتبطة بانتهاكات الأمن السيبراني بشكل مرتفع ومتزايد، ففي الولايات المتحدة زادت تكاليف برامج الفدية من ٢٥ مليون دولار في عام ٢٠١٤ إلى أكثر من ٨ مليارات دولار في عام ٢٠١٨، ونظراً للطبيعة المتفشية والتكاليف الكبيرة المصاحبة لحوادث الأمن السيبراني، أصبح الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات العامة وكيفية إدارة هذه المخاطر ذات أهمية متزايدة لأصحاب المصلحة، ونظراً لأن الشركات العامة تسعى بشكل متزايد إلى تقديم إفصاحات طوعية لفحص الأمن السيبراني، فمن غير الواضح كيف سيتصور المستثمرون هذه الإفصاحات.Morgan, S. (2018)

وتتزايد المخاطر والتهديدات المرتبطة بانتهاكات الأمن السيبراني بشكل مرتفع، ونظرا للطبيعة المنتشرة والتكاليف الكبيرة المصاحبة لحوادث الأمن السيبراني أشارت دراسة Hinz, O., et al. (2015) إلى أن حوادث الأمن السيبراني يمكن أن تكون مكلفة من حيث جهود الإصلاح، وتعطل النظام، وفقدان السمعة والثقة، ويعد هذا هو السبب المحتمل وراء إشارة الدراسات السابقة Kamiya, S., et al., (2020) لرد فعل سلبي للسوق على حوادث الأمن السيبراني المفصح عنها، كما تؤدى حوادث الأمن السيبراني عادةً إلى خسارة في القيمة السوقية للشركات المتضررة ففي الحالات القصوى يمكن أن يصل الانخفاض في القيمة السوقية للشركة إلى ١٢ ٪ خلال فترة يومين بعد الاختراق، كما يمكن أن تنعكس الحوادث السيبرانية أيضاً في هوامش العرض والطلب الأوسع وحجم التداول غير الطبيعي.

فلقد أدى اختراق وكالة Equifax لإعداد التقارير الائتمانية ٢٠١٧ إلى انخفاض سعر سهم الشركة بنسبة ١٨٪ تقريباً عند الإفصاح الأول عن الاختراق، وأشارت وثائق المحكمة المقدمة لتسوية القضية إلى أن الحد الأدنى للتكلفة ١,٣٨ مليار دولار أمريكي،

ولذلك شكل هذا الهجوم على الشركة أحد أكبر المخاطر على المعلومات الحساسة شخصياً في السنوات الأخيرة(Bernard et al. (2017 ، الأمر الذى يوضح مدى تأثير هجمات الأمن السيبراني على القيمة السوقية لأسعار الأسهم وما يترتب على ذلك من انخفاض كبير وخسائر هائلة، حيث أوضح Corbet, S. & C. Gurdgiev. (2019) أن الجرائم الإلكترونية تؤثر بشكل كبير على تقلبات سوق الأسهم .

وأوضحت دراسة Bourdon, B. (2019) أن مرتكبي الهجمات الإلكترونية يخترقون الأمن السيبراني للشركات بشكل متكرر ويسرقون البيانات السرية للحصول على مزايا مالية سريعة وغير قانونية، ويتضح ذلك من خلال سلسلة الاختراقات التي تعرضت لها شركة Yahoo Inc في أواخر عام ٢٠١٦عندما تمكن أحد المتطفلين من الوصول إلى شبكة الشركة وسرقه معلومات من حسابات ما لا يقل عن ٥٠٠ مليون مستخدم، وأشارت دراسة Rosati, P., et al. (2019) إلي اختراق ثان للبيانات في ١٤ ديسمبر ٢٠١٦ لشركة Yahoo Inc فبصورة مماثلة للاختراق السابق تم اختراق حسابات ثلاثة مليارات مستخدم، وهو ما يمثل حتى الآن أكبر اختراق للبيانات في التاريخ، وفى الواقع فإن حقيقة أن شركة تكنولوجيا كبيرة مثل شركة Yahoo Inc، استغرقت أكثر من عامين للكشف عن عمليات الاختراق وتأكيدها وكذلك لتقدير عدد السجلات المسروقة توفر فكرة عن مدى تعقيد هذه العمليات وصعوباتها.

ووفقاً لما أوضحته دراسة Perols, R. R., & Murthy, U. S. (2021) فإنه ينظر إلى مخاطر الأمن السيبراني بشكل متزايد على أنها واحدة من أهم التحديات التي تواجه الشركات في الولايات المتحدة، ويمكن أن تؤدي الجرائم الإلكترونية إلى الإضرار بالسمعة وفقدان الملكية الفكرية وتعطيل العمليات التجارية والغرامات الحكومية ونفقات التقاضي، حيث تجد الشركات التي تعاني من حوادث الأمن السيبراني نفسها تواجه العديد من التكاليف المباشرة وغير المباشرة وغير المتوقعة، وتشمل التكاليف المباشرة تكاليف الإصلاح والأتعاب القانونية والغرامات والمعاملات المفقودة، فقد تم تغريم Choice Point بمبلغ ١٠ ملايين دولار وكان عليها دفع ٥

ملايين دولار أخرى لتعويض الأفراد المتضررين ، وبالمثل عانت Nasdaq & BATS من هجوم إلكتروني على مدار ٢٤ ساعة على موقع الويب الخاص بهما مما أدى إلى انخفاض بنسبة ١٢% في نشاط التداول اليومي في الولايات المتحدة Dennis, A., et al. (2015).

فيما تشمل التكاليف غير المباشرة خسارة الإيرادات الحالية والمستقبلية بالإضافة إلى تدهور ثقة العملاء والشركاء وهذه التكاليف بحكم تعريفها يصعب تقديرها، لذلك فإنها تتضمن درجة معينة من حرية التصرف والتي قد تزيد في النهاية من المخاطر التي يتعرض لها المراجع الخارجي، كما أشارت دراسة Dennis, A., et al. (2015) أيضاً إلى أن التكاليف غير المباشرة المرتبطة بالحوادث السيبرانية (الأعمال المفقودة بشكل أساسي) أكبر بكثير من (ضعف) التكاليف المباشرة مثل تكاليف حل البيانات أو الاستثمارات في التقنيات أو الأتعاب القانونية، لذلك على الرغم من أن التكاليف المباشرة للحادث السيبراني قد لا تكون جوهرية، إلا أن التكاليف غير المباشرة الناتجة قد تكون جوهرية بما يكفي لتوفير حوافز إدارية لتحيز التقرير المالي، ولهذا يقوم المراجع بإجراءات مراجعة أكثر تكلفة لتحقيق مستوى مقبول من مخاطر المراجعة وقد يفرضون علاوة أتعاب إذا كان الجهد الإضافي غير كافٍ لتغطية التكاليف المتبقية في ظل مخاطر الأعمال المتزايدة للعميل.

وتوضح دراسة (فرج ،٢٠٢٢) وجود ارتفاع كبير في الدعاوى القضائية المرفوعة ضد مجالس إدارات الشركات الحادث بها اختراقات إلكترونية، مما يعنى زيادة المسئوليات على الإدارة بعد حدوث الاختراقات، خاصة وأن هذه الاختراقات يترتب عليها الإضرار بسمعة الشركة، وفقدان الملكية الفكرية، وتعطيل العمليات الرئيسية، ووجود غرامات وعقوبات لتكاليف التقاضي، لذلك تحتاج الإدارة لأدوات تساعدها على مواجهة هذه المخاطر الجديدة لمساعدتها على الوفاء بمسئولياتها، وفى الوقت نفسه يحتاج أصحاب المصلحة إلى معلومات مفيدة في الوقت الملائم حول جهود الإدارة لتفادى مخاطر الأمن الإلكتروني بالشركة، الأمر الذى يؤدى إلى إلقاء

مهام إضافية على المراجع الخارجي للحصول على المزيد من التأكيد حول تأثير تلك المخاطر على قيمة الشركة.

كما يؤكد الباحثان علي أن ما ينتج عن هجمات الأمن السيبراني من مخاطر تؤثر وبشكل مباشر على قيمة الشركة بل وتمتد إلى التأثير على قدرتها التنافسية وبقاؤها، وما يترتب على ذلك من تكاليف غير مباشرة قد تتمثل في فقدان فرص العمل، خفض الإيرادات، وفقد ثقة العملاء يصعب تحديد كميتها بشكل موضوعي، إنما تمثل تحدياً كبيراً لكافة الأطراف المتعلقة بالمنشأة، وتشمل درجة أكبر من مخاطر عملية المراجعة تتطلب من المراجع المزيد من الجهد المبذول عن مدى تأثير هذه الهجمات على قيمة الشركة الأمر الذى يعد خارج نطاق عمل المراجع ويصنف على أنه خدمات إضافية يقابلها المزيد من الجهد الذى ينعكس بدوره على ارتفاع أتعاب المراجع الخارجي.

٢- ٢ الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ظل الاهتمامات الدولية كمرتكز للمراجع الخارجي

لقد زاد الإفصاح عن مخاطر الأمن السيبراني للشركات بشكل كبير على مر السنين وهو مدفوع بعوامل كثيرة مثل زيادة مخاطر الأمن السيبراني، وتوجيهات هيئة البورصة الأمريكية وحجم الشركة، وفى هذا السياق تناقش دراسة Haapamaki, E.,&Sihvonen, J. (2019) بأن الشركات لا يجب أن تقوم فقط بتثبيت برامج فعالة لإدارة المخاطر الإلكترونية ولكن أيضاً توفر معلومات مفيدة وفي الوقت المناسب حول مثل هذه المبادرات لأصحاب المصلحة من خلال تقارير الأمن السيبراني، فأوضحت دراسة Bourdon,B. (2019) أن مرتكبي الهجمات الإلكترونية يخترقون الأمن السيبراني للشركات بشكل متكرر ويسرقون البيانات السرية للحصول على مزايا مالية سريعة وغير قانونية، ومن ثم تزايد الطلب من جانب أصحاب المصلحة لمزيد من الشفافية من الشركات العامة لتوضيح كيفية تحديد وقياس وإدارة المخاطر الإلكترونية، وأن الإفصاح عن الأمن السيبراني يعد أجندة

جديدة نسبياً لإفصاحات الشركات، ونظراً للطبيعة البارزة للهجمات الإلكترونية على الشركات، فقد نما الطلب على المعلومات المتعلقة بالأمن السيبراني والحاجة إلى تسهيل المحادثات القوية حول هذه الموضوعات بشكل كبير عبر مجموعات أصحاب المصلحة الرئيسيين، وغالباً ما تسلط وسائل الإعلام الإخبارية الرئيسية الضوء على القلق بشأن الهجمات الإلكترونية.(2018) .Pendley, J. A

ولمعالجة القلق المتصاعد بشأن مخاطر الهجمات الإلكترونية، يجب على كل شركة ضمان حوكمة قوية للأمن السيبراني وتقديم إفصاحات كافية حول كيفية تحديد أولويات الأمن السيبراني وإدارته، حيث ذكرت دراسة .Berkman, H., et al (2018) وجود ارتباط إيجابي بين الإفصاح الاختياري لأمن المعلومات والقيمة السوقية، كما ناقشت أن الشركات العامة يجب أن تفهم أهمية الأمن السيبراني وتسعى للإفصاح المناسب حول هذه المسألة، حيث ستسمح مثل هذه الإفصاحات للشركات بإثبات مسؤوليتها ومشاركتها في هذه القضية وبناء ثقة أصحاب المصلحة.

وكجزء من مسؤولياتهم الرقابية من المتوقع أن يصبح أعضاء مجلس الإدارة أكثر اندماجاً وأن يضطلعوا بدور استباقي لفهم وإدارة مخاطر الأمن السيبراني في جميع أنحاء الشركة (2021) .Mohan, V., et al ، إضافة إلى دورهم المنتظر في توفير إفصاح كافٍ وذو صلة بالأمن السيبراني والذى يوفر أيضاً الشفافية حول كيفية وفاء مجالس الإدارة بمسؤولياتها المتعلقة بالإشراف على مخاطر الأمن السيبراني، حيث أن حوادث الأمن السيبراني اللاحقة التي تحدث بعد إصدار تقرير فحص الأمن السيبراني يمكن أن توفر إشارة خارجية سلبية للمستثمرين حول جودة التأكيد الخارجي، فإذا تم توفيرها بشكل منفصل يجب أن توفر حادثة الأمن السيبراني اللاحقة إشارة سلبية لجودة فحص الأمن السيبراني نظراً لأن فحص الأمن السيبراني لا يتم إجراؤه بواسطة شركة المراجعة. ومع ذلك عندما يتم توفير فحص الأمن السيبراني بشكل مشترك، يمكن أن تقلل الإشارة أيضاً من تصورات المستثمرين لجودة أعمال المراجعة المتكاملة، وبشكل أكثر تحديداً، قد تؤدى حادثة الأمن السيبراني اللاحقة إلى

إرسال إشارة سلبية لجودة التأكيد الخارجي مما يزيد من حساسية المستثمرين تجاه إعاقات الاستقلال المحتملة وتقليل تصورات المستثمرين عن كفاءة المراجع ,Perols .R. R., & Murthy, U. S. (2021)

لذا يفصح المديرون عن المزيد من عوامل الخطر ويخصصون جزءاً أكبر من إفصاحاتهم لهذه العوامل عندما تكون المخاطر أعلى وأكثر أهمية، ومع ذلك أدت قاعدة الإفصاح لعام ٢٠١١ الصادرة عن هيئة البورصة الأمريكية إلى زيادة عمليات الإفصاح عن مخاطر الأمن السيبراني للشركات بغض النظر عن درجة مخاطر الأمن السيبراني، ونظراً لأن الشركات ليست محصنة ضد المخاطر الإلكترونية، فقد تستخدم التأمين الإلكتروني للتخفيف من الخسائر المالية المحتملة، وهذه التغطية ليست جديدة فقد تمت الإشارة إلى عام ١٩٩٨ باعتباره العام الذي تم فيه تقديم التأمين الإلكتروني لأول مرة. وأصبحت منتجات التأمين الإلكتروني اليوم أكثر تعقيداً بسبب زيادة التنظيم والتهديدات الأكثر تعقيداً، حيث تكون التغطية التأمينية ضد إتلاف البيانات والسرقة والقرصنة والابتزاز، بالإضافة إلى تغطية الأعمال التجارية المسئولة عن أمان العملاء عبر الإنترنت ضد الأخطاء أو الإغفالات التي تنشأ عن تقديم الخدمة. Pacheco-Paredes, A., & Wheatley, C. M. (2022)

فيما يكون التأثير على شركات التأمين من جانبين، فمن ناحية يؤدي الإفصاح عن انتهاكات الأمن السيبراني بشكل ميكانيكي إلى دفع تعويضات على بوليصة التأمين المعنية و(يحتمل) زيادة الاحتمالية المقدرة لاستحقاق المدفوعات المستقبلية مع وجود المزيد من الشركات، ومن ناحية أخرى يمكن أن يؤدي التهديد المتزايد للهجمات الإلكترونية إلى زيادة الطلب على منتجات شركة التأمين(2019) ,.Haislip, J .

بينما وجد Lawrence, Minutti-Meza, and Vyas (2018) أن اختراقات البيانات مرتبطة بنقاط ضعف في الرقابة المالية في المستقبل، فإن أتعاب المراجعة تعكس أكثر من مجرد مخاطر المراجعة، حيث تعكس أيضاً تصورات المراجع

لمخاطر الأعمال التجارية للعميل، فالشركات التي تشتري التأمين الإلكتروني ستكون في حد ذاتها هي تلك التي لديها مخاطر أعمال مالية أعلى ومن المحتمل أن يتم تسعير مخاطر الأعمال في أتعاب المراجع (أي أتعاب أعلى لمشتري التأمين الإلكتروني مقارنة بالشركات التي لديها ملفات تعريف منخفضة المخاطر). ونظراً لأن المراجع (من خلال فحص المعاملات) سيعرف بوجود مثل هذا التأمين، فمن المحتمل أن تكون أقساط المخاطر للشركات المؤمن عليها أقل من تلك الشركات التي لديها ملفات تعريف مخاطر مماثلة بدون تأمين إلكتروني، وسيكون هذا صحيحاً بالنسبة لجميع الشركات التي تشتري التأمين الإلكتروني سواء تم الإفصاح عنه أم لا وسواء حدث اختراق أم لا.

واستناداً إلى ما سبق ركزت الهيئات التنظيمية في الولايات المتحدة الأمريكية وكندا في السنوات الأخيرة الضوء أيضاً على أهمية عمليات الإفصاح عن الأمن السيبراني وقدمت إرشادات مفصلة، ونظراً لأن الشركات العامة تسعى بشكل متزايد إلى تقديم إفصاحات طوعية لفحص الأمن السيبراني، فمن غير الواضح كيف سيتصور المستثمرون هذه الإفصاحات، واهتمت هيئة البورصة الأمريكية (SEC) بشكل خاص بتهديدات الأمن السيبراني التي تواجه المستثمرين غير المحترفين (الأفراد) والحاجة إلى إفصاحات أكثر قوة للأمن السيبراني، بما في ذلك مزيد من المعلومات حول برامج إدارة مخاطر الأمن السيبراني للمؤسسات والإجراءات الوقائية المتخذة لإدارة مخاطر الأمن السيبراني (Perols, R. R., & Murthy, U. S. (2021.

وفي عام ٢٠١١ أصدرت هيئة البورصة الأمريكية توجيهها الأول بشأن التزامات الإفصاح المتعلقة بمخاطر وحوادث الأمن السيبراني لمساعدة الشركات في تقييم ما يجب أن تقوم به من إفصاحات في هذا المجال إن وجدت وتنص التوجيهات على أنه في حين لم يتم فرض متطلبات إفصاح صريحة تتعلق بمخاطر الأمن السيبراني والحوادث الإلكترونية فإن الإفصاح عن مخاطر وقضايا الأمن السيبراني يتفق مع مشاركة المعلومات الدقيقة في الوقت المناسب للمساعدة في اتخاذ قرارات

الاستثمار(Barry, T.et al. (2022 ، كما نصت التوجيهات بأنه "على الرغم من عدم وجود شرط إفصاح حالي يشير صراحة إلى مخاطر الأمن السيبراني والحوادث الإلكترونية، إلا أن عدداً من متطلبات الإفصاح قد تفرض التزاماً على المسجلين بالإفصاح عن مثل هذه المخاطر والحوادث"، ووفقاً للإرشادات يعتمد مستوى ونوع الإفصاح على حقائق الشركة وظروفها بما في ذلك احتمالية الهجمات الإلكترونية وحجم أي تأثير على الشركة.

وفي فبراير ٢٠١٨ بعد اختراق Equifax عام ٢٠١٧ واختراق قاعدة بيانات EDGAR عام ٢٠١٧ حدثت هيئة البورصة الأمريكية إرشاداتها لعام ٢٠١١ وتوسيعها لتقديم المزيد من المساعدة للشركات في إعداد الإفصاحات حول مخاطر وحوادث الأمن السيبراني، ويستند التوجيه الجديد إلى إرشادات الأمن السيبراني الصادرة عن SEC لعام ٢٠١١ والتي أوضحت التزامات الشركات بالإفصاح عن مخاطر الأمن السيبراني والانتهاكات المادية والتأثير المحتمل لهذه الانتهاكات، وقد تم تناول موضوعين في إرشادات ٢٠١٨ لم يتم تطويرهما في إرشادات عام ٢٠١١ على النحو التالي :

١- أعادت التوجيهات الجديدة التأكيد على أهمية إجراءات الأمن السيبراني: حيث أكدت إرشادات عام ٢٠١٨ على أهمية إجراءات وضوابط الأمن السيبراني لتمكين الإفصاح عن مخاطر وحوادث الأمن السيبراني في الوقت المناسب وبدقة.

٢- أوضحت إرشادات ٢٠١٨ أن التداول من الداخل لحوادث الأمن السيبراني محظور: وتتطلب الإرشادات من الشركات الامتثال لقوانين التداول من الداخل فيما يتعلق بأي معلومات حول حوادث الأمن السيبراني، ويجب أن يكون لدى الشركات إجراءات وسياسات قائمة لمنع التداول بناءً على مخاطر وحوادث الأمن السيبراني.

ويوضح الباحثان أن توفير إطار عمل لمراجعة الإفصاح عن مخاطر الأمن السيبراني يوفر لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للشركة وفعالية برنامج إدارة المخاطر الخاص بها، حيث أشارت دراسة (فرج،٢٠٢٢) إلى أن دليل إرشادات الإفصاح عن الأمن السيبراني الصادر عن هيئة البورصة الأمريكية يشتمل على :

١- **المجموعة الأولى**: مراجعة قواعد الإفصاح عن مشاكل الأمن السيبراني تشمل :

- الأهمية النسبية: من خلال التركيز على مخاطر وحوادث الأمن السيبراني عند إعداد تقارير الإدارة السنوية، وخاصة الحوادث الهامة من وجهة نظر المستثمرين والأضرار الناتجة عنها، كما يجب أن يستوفى الإفصاح خاصيتي الملاءمة والاكتمال عند الإفصاح عن إدارة مخاطر الأمن السيبراني.
- عوامل المخاطرة: يجب أن يشمل الإفصاح عن حوادث الأمن السيبراني الفعلية والمتوقعة والتي تمثل مخاطر خاصة على الشركة في سياق الإفصاح عن إدارة مخاطر الأمن السيبراني للمستثمرين.
- المركز المالي ونتائج الأعمال: يجب الإفصاح عن أي حوادث أمن سيبراني يكون لها تأثير جوهري على المركز المالي ونتائج الأعمال.
- وصف طبيعة الأنشطة: يجب الإفصاح عن أي حوادث أمن سيبراني يكون لها تأثير جوهري على طبيعة نشاط الشركة والعلاقات مع الموردين أو العملاء أو أي أطراف خارجية أخرى.
- الإجراءات القانونية : تشمل الإفصاح عن أي قضايا متعلقة بإدارة مخاطر الأمن السيبراني
- سياسات الإفصاح في القوائم المالية: قد تؤثر على حوادث الأمن السيبراني على عناصر القوائم المالية من إيرادات أو مصروفات أو تدفقات نقدية، وبالتالي لابد من الإفصاح عن هذه الأثار ضمن الإيضاحات المتممة للقوائم المالية .

- دور مجلس الإدارة : يجب الإفصاح عن دور مجلس الإدارة بخصوص برنامج إدارة مخاطر لأمن السيبراني والذى يؤثر إيجاباً على المستثمرين .

٢- **المجموعة الثانية**: السياسات والإجراءات الخاصة بالرقابة على الإفصاح عن إدارة مخاطر الأمن السيبراني وتشمل:

- إجراءات الرقابة: يجب التأكد من وجود تصميم جيد لضوابط وإجراءات الرقابة على برنامج إدارة مخاطر الأمن السيبراني المطبق بالشركة فهي جزء من أعمال لجنة المخاطر بالشركة.
- المعلومات الداخلية: يجب أن لا يستغل الأطراف الداخلية معرفتهم بأحداث جوهرية حول مخاطر الأمن السيبراني المطبق بالشركة فهي جزء من أعمال لجنة المخاطر بالشركة.
- الإفصاح الانتقائي: يجب عد الإفصاح عن المعلومات المتعلقة بإدارة مخاطر الأمن السيبراني بشكل انتقائي وهى المعلومات غير المعلنة للمستثمرين.

وأشارت دراسة Frank, M. L., et al. (2019) إلى أن AICPA بالتعاون مع مجلس معايير المراجعة قد طور إطار عمل طوعي لإعداد تقارير إدارة مخاطر الأمن السيبراني والتأكيد، كما أشار في دراسته Yang, L., Lau, L., & Gan, H. (2020) إلي أن AICPA, 2017 قام بتطوير إطار عمل لإعداد تقارير إدارة مخاطر الأمن السيبراني لتوجيه الشركات في تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني، ويمكن استخدامها للإفصاح عن المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته، على وجه التحديد اقترح إطار العمل ثلاث أجزاء رئيسية من المعلومات تهدف إلى مساعدة أصحاب المصلحة في مراقبة برنامج إدارة مخاطر الأمن السيبراني للشركة:

١- وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للشركة، حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة ، وتزويد المستخدمين

المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة.

٢- تأكيد الإدارة بشأن فعالية ضوابط الأمن السيبراني، وأنها تتوافق مع معايير AICPA وأن الضوابط التي تنفذها الإدارة يمكن ان تحقق أهداف الأمن السيبراني للشركة بشكل فعال، وتستند هذه الأهداف إلى مجموعة من معايير الرقابة المناسبة مثل معايير خدمات الثقة (الأمان، التوافر، السرية).

٣- رأي المراجع في إفصاحات الإدارة وفعالية ضوابط الشركة (تقرير ضوابط النظام والتنظيم للأمن السيبراني).

وعلى ذلك فإن الإفصاح عن مخاطر الأمن السيبراني في تقرير المراجع يوضح مستوى وعي الإدارة بقضايا أمن نظم المعلومات والخطوات الاستباقية التي يتخذونها لحماية النظام المالي، واكتشاف التهديدات، والاستجابة لقضايا الأمن السيبراني بشكل مناسب في الوقت المناسب، على وجه التحديد يشمل دور المراجعين سياقين مهمين: مراجعة البيانات المالية والرقابة الداخلية على التقارير المالية (ICFR) ، والإفصاحات بناءً على معايير المراجعة الحالية، حيث يحتاج مراجعي الحسابات إلى فهم كيفية استخدام الشركات لتكنولوجيا المعلومات (IT) وتأثير تكنولوجيا المعلومات على البيانات المالية، ويكون المراجع مطالب أيضاً بفهم العملية الآلية والضوابط من حيث صلتها بالتقارير المالية، كما يحتاج مراجعي الحسابات إلى تقييم مخاطر التحريف الجوهري الناتج عن القضايا المتعلقة بالأمن السيبراني، فعندما يتم تحديد خرق إلكتروني يحتاج المراجع إلى تقييم تأثيره على البيانات المالية وتأثيره على ICFR Calderon, T. G., & Gao, L. (2021).

٢-٣ تفسير العلاقة بين الإفصاح عن الأمن السيبراني وأتعاب المراجع الخارجي

لقد أثار الاتجاه التصاعدي لانتهاكات أمن المعلومات مناقشة حول أهمية فهم المراجعين لبيئة تكنولوجيا المعلومات للعملاء، فقد أصدر مركز جودة المراجعة (CAQ) تنبيهاً لما يقرب من ٦٠٠ من أعضاء شركات المراجعة التابعة له يلخص

واجبات المراجعين الخارجيين فيما يتعلق بالأمن السيبراني، بشكل عام يُطلب من المراجعين فهم بيئة العميل، مثل الظروف الاقتصادية، المتطلبات التنظيمية، البيئة التنافسية، التطورات التكنولوجية، والرقابة الداخلية والتقرير عن فعالية الرقابة الداخلية على أنظمة المعلومات (Yen, J. C., et al. (2018.

وبحسب ما أشارت إليه دراسة Yen, J. C., et al. (2018) أن هذا الفهم قد يكون بالغ الأهمية لأن تكنولوجيا المعلومات (IT) من ناحية تعزز توقيت المعلومات ودقتها بالإضافة إلى تقليل فرصة التحايل على الضوابط وكلاهما يقلل من احتمالية التحريف والاحتيال، ومن ناحية أخرى تشكل تكنولوجيا المعلومات أيضاً مخاطر تتعلق بأمن المعلومات، مثل الوصول غير المصرح به إلى البيانات، أو تدمير البيانات أو إجراء تغييرات غير مناسبة عليها، أو عدم توفر البيانات للاستخدام المصرح به، مما يؤثر بشكل كبير على المنظمات ويؤثر على موثوقية التقارير المالية وفعالية وكفاءة العمليات المرتبطة بمخاطر التقارير المالية، كما ينعكس في المزيد من إعادة التصريحات وخطابات تعليقات هيئة البورصة الأمريكية، وبالتالي لتقليل مخاطر المراجعة مسبقاً يكون من المهم أن يعطى المراجع الخارجي الوقت والجهد لفهم وتقييم مخاطر أمن معلومات العملاء، ومع ذلك فإن مدى الوقت والجهد المبذول من قبل المراجع قد يكون مشروطًا بالعديد من خصائص شركة المراجعة، مثل المعرفة المحددة حول الصناعة، والإلمام بعمليات العميل، والموارد اللازمة لفهم مخاطر أمن المعلومات.

وفى هذا السياق توضح دراسة Hansen, J. C. (2022) أن عوامل الخطر على مستوى العميل تدفع أتعاب المراجعة مثل حجم العميل والتعقيد والأشكال المختلفة للمخاطر والتي منها مخاطر إدارة الأرباح والمخاطر المالية ومخاطر حوكمة الشركات. ويشير Prabhawa, A. A., & Nasih, M. (2021) إلي أن أتعاب المراجعة هي جميع أتعاب خدمات المراجعين المقدمة من قبل مكاتب المراجعة، ويتأثر مبلغ أتعاب المراجعة بحجم شركة العميل ومدى تعقيد عملية المراجعة ومخاطر المراجعة، ويكون هناك حاجة إلى مستوى أعلى لضمان بذل جهد أكبر لمواجهة مخاطر أعلى، ويمكن أن

تكتشف جودة المراجعة المرتفعة المزيد من الأخطاء مما يؤدى إلى عدد أقل من التحريفات، كما ذكرت دراسة Zhou, X. (2022) أن أتعاب المراجعة تمثل المكافأة الضرورية لمراجعي الحسابات لتقييم المخاطر وإتمام أعمال المراجعة وهي نفقات ضرورية لتقييم جودة المعلومات المحاسبية للشركة.

وتعرف نظرية تسعير المراجعة كأساس لتحديد تكلفة المراجعة (أتعاب المراجعة)، حيث يتم قياس أتعاب مراجع الحسابات باستخدام الكمية (Q) من خلال حساب المبلغ باستخدام ساعات عمل المراجع، والسعر(P) من خلال متوسط معدل الفواتير لساعات العمل، ولذا يوضح Prabhawa, A. A., & Nasih, M. (2021) أن هناك نوعان من وجهات النظر عند تحديد أتعاب المراجعة وهما جانب الطلب والعرض، ويشير منظور أتعاب المراجعة من جانب الطلب إلى وجود علاقة إيجابية بين جودة حوكمة الشركات وتكاليف المراجعة، حيث أن أتعاب المراجعة تميل إلى الارتفاع استجابةً للمخاطر العالية للتحريف وطلبات المراجعة عالية الجودة من قبل الحوكمة لحماية رأس مال سمعتها، تميل المجالس ذات الخبرة إلى البحث عن عمليات مراجعة أعلى جودة من المراجعين الخارجيين؛ وهذا يشجع المراجعين على فرض أتعاب أعلى.

كما توضح دراسة Mitra, S., et al. (2019) أن طلب المراجعة يمثل وظيفة لمجموعة المخاطر التي يواجهها أصحاب المصلحة في المنظمة ومجموعة آليات الرقابة لتقليل هذه المخاطر، ومن منظور جانب العرض تظهر علاقة سلبية بين جودة حوكمة الشركات وتكاليف المراجعة، حيث يمكن أن تقلل الضوابط الأكثر صرامة وبيئة الحوكمة من تقييم المراجع لمخاطر الرقابة ومستوى إجراءات المراجعة، وبالتالي تقليل تكاليف المراجعة وتوجد علاقة مهمة وإيجابية بين تعقيد العميل وتكاليف المراجعة الخارجية لأن المراجعين الخارجيين سيحتاجون إلى مزيد من الوقت للمراجعة والمزيد من الخبرة للمراجعة عندما تكون الشركة العميلة أكثر تعقيداً من الشركة العميلة الأقل تعقيداً.

وتشير دراسة Smith, D. D., et al. (2021) إلى أن نموذج أتعاب المراجعة يوضح العوامل المسعرة من قبل المراجعين والناشئة عن تعاملهم مع العميل وأن المراجعين ينشئونها عن ارتباطهم مع العميل، حيث تتكون أتعاب المراجعة من عنصرين هما(تكلفة إجراء المراجعة، واحتمال أن يضطر المراجع إلى دفع ثمن الخسائر المنسوبة إلى عميل المراجعة)، وقد تنشأ المخاطر التي تواجه شركات المراجعة من إخفاقات المراجعة والمخاطر من ارتباطها بعميل المراجعة، وكلاهما يمكن أن يؤدي إلى رفع دعوى قضائية ضد المراجع، حتى مطالبات المسؤولية الضعيفة قد تستغرق أكثر من ثلاث سنوات للتقاضي بتكلفة متوسطها ٣,٧ مليون دولار لكل مطالبة، ويوضح Ahmad, F., et al (2021) في دراسته أن المراجعين يمكنهم تقليل مخاطر المراجعة الإجمالية إما عن طريق زيادة الموارد (أي عن طريق زيادة اختبار المراجعة من خلال المزيد من ساعات المراجعة أو المراجعين الأكثر خبرة) أو عن طريق فرض أتعاب مراجعة إضافية.

ولهذا يوضح Hossain, S., & Wang, J. J. (2022) أن أتعاب المراجعة الفعلية تشمل مكونات الأتعاب العادية وغير العادية، حيث يتم تحديد الأتعاب العادية بشكل أساسي من خلال العوامل المشتركة بين العملاء المختلفين، مثل حجم العميل وتعقيد العميل والمخاطر الخاصة بالعميل، بينما أتعاب المراجعة غير العادية يتم تحديدها من خلال عوامل خاصة بعلاقة محددة بين المراجع والعميل. وحيث تشير دراسة Muniandy, B. (2022) إلى أن أتعاب المراجعة تمثل المكافآت المدفوعة للمراجعين الخارجيين مقابل خدمات المراجعة التي يقدمونها، فإن أتعاب المراجعة هي وظيفة مكونين رئيسيين، وهما تكاليف الموارد والتي تنشأ من أداء المزيد من أعمال المراجعة، والخسائر المستقبلية المتوقعة والتي تنشأ من مخاطر التقاضي، وتناقش الدراسة أن أتعاب المراجعة من المعروف أنها تختلف اختلافاً كبيراً حسب الحجم والتعقيد والمخاطر والخصائص الأخرى للكيان الخاضع للرقابة.

وتوصلت دراسة Lim, Y., & Monroe, G. S. (2022) إلى أن التطبيق الإلزامي للمعايير الدولية لإعداد التقارير المالية أدى إلى زيادة أتعاب المراجعة خلال سنة التطبيق وفي السنوات اللاحقة، ويشير هذا إلى أن زيادة تعقيد مهام المراجعة المرتبطة بتبني المعايير الدولية لإعداد التقارير المالية تمثل القوة الدافعة الرئيسية للتغيير في أتعاب المراجعة، إضافة إلى أن علاوة المراجعة المتعلقة بالمعايير الدولية لإعداد التقارير المالية تتناقص مع التحسينات في جودة التقارير المالية التي أحدثها اعتماد المعايير الدولية للتقرير المالي، ومع قوة النظام القانوني للدولة، وأن كلاً من ضغوط التقاضي المتزايدة، التقاليد المؤسسية للإفصاح المتزايد، والتنظيم المتزايد يمارس ضغوطًا تصاعديه على أتعاب المراجعة، وأن قوة نظام المسئولية القانونية للدولة له ارتباط إيجابي بأتعاب المراجعة ويحدث هذا لأنه عندما يصبح النظام القانوني أقوى فمن الأكيد أن يتحمل المراجع المسئولية القانونية في حالة فشل المراجعة، مما يؤدي إلى بذل المراجعين مزيداً من الجهد وفرض أتعاب مراجعة أعلى للتعويض عن الاحتمال المتزايد للمراجعة القانونية.

فمن وجهة نظر المراجع فإن الخسارة المتوقعة من الارتباط بعميل محفوف بالمخاطر تزيد من مخاطر أعمال المراجع مثل ضعف السمعة وعدم تحصيل الأتعاب، ولذا فإن شركات المراجعة تأخذ في الاعتبار مخاطر الأعمال في عمليات تسعير المراجعة وأن الشركات تفرض أتعاب مراجعة إضافية عندما تكون مخاطر العمل عالية، فالإشارة الأساسية لإدراك المراجعين مخاطر أعمال العميل والتفاعل معها هي قيامهم بإضافة هذه المخاطر في أتعاب المراجعة، وحيث يقدم المراجع ضماناً موضوعياً ومستقلاً فيما يتعلق بجودة التقارير المالية للشركة وهم مسئولون عن مراجعة البيانات المالية والرقابة الداخلية على التقارير المالية (ICFR) Kajüter, P., et al (2016) & Rosati, P., et al. (2017) فإن مراجع الحسابات يوفر تأكيداً لأصحاب المصلحة الخارجيين حول جودة وموثوقية المعلومات الواردة في القوائم المالية لعملائهم، حيث تضمنت مسئوليات المراجعين الصادرة عن مركز جودة المراجعة بشأن الأمن السيبراني أن يكون المراجع مسئولاً عن تقييم

محاسبة الشركة للخسائر المتعلقة بالأمن السيبراني، وتقييم التأثير على القوائم المالية للشركة والإفصاحات، وفحص ضوابط الشركة المتعلقة بالتسجيل في الوقت المناسب والإفصاح عن المعلومات الضرورية في البيانات المالية.

وفيما يلى يعرض الباحثان العلاقات التأثيرية المتبادلة بين مخاطر الأمن السيبراني وجوهر وأتعاب عملية المراجعة من خلال :

٢-٣-١ الإفصاح عن مخاطر الأمن السيبراني في ضوء تحليل المحتوى

تمثل حوادث الأمن السيبراني مخاوف حقيقية لمراجعي الحسابات، وعلى هذا النحو فإن الإفصاح عن حادثة الأمن السيبراني يزيد من المخاطر التي يتعرض لها المراجع الخارجي، ويؤدي هذا عادةً إلى زيادة جهد عملية المراجعة، الأمر الذي يترجم في النهاية إلى أتعاب مراجعة مرتفعة، ولقد وثقت الدراسات السابقة Spanos Kamiya, S., et ؛ Rosati, P., et al(2017) ; & Angelis, (2016) al.(2018) الآثار المترتبة على حوادث الأمن السيبراني على مستوى الشركة والسوق وفى هذا السياق ذكرت دراسة **(**Calderon, T. G., & Gao, L. (2021 أن أتعاب المراجع الخارجي تتأثر بمحتوى (عدد الكلمات)، باللغة (سهولة القراءة) التي تم استخدامها في عمليات الإفصاح عن مخاطر الأمن السيبراني.

وأوضحت دراسة Calderon, T. G., & Gao, L. (2021) أن دور المراجعين فيما يتعلق بمخاطر الأمن السيبراني يشمل تقييم إفصاحات الأمن السيبراني في نموذج إفصاح الشركات (K-10) مما يعنى بذل جهد أكبر من قبل المراجعين لتقييم الآثار المترتبة على مخاطر المراجعة، وبالتالي يمكن للمراجع أن يقيم مخاطر الأمن السيبراني من خلال نماذج الإفصاح، فقد يوجد ارتباط إيجابي بين عدد الكلمات التي تكشف عن مخاطر الأمن السيبراني وأتعاب المراجعة ، كما تشير قابلية التقارير للقراءة وهي خاصية أخرى للإفصاحات إلى مدى السهولة التي يمكن للقارئ من خلالها فهم النص المكتوب، فلقد تم التأكيد على إفصاحات اللغة الإنجليزية المبسطة وسهولة القراءة من قبل هيئة البورصة الأمريكية لتشجيع الإفصاحات سهلة القراءة، فنماذج الإفصاح التي يصعب

قراءتها تكون معقدة وتنقل احتمالية وجود مخاطر كامنة ومخاطر رقابة أعلى، لذلك يجب على المراجع بذل جهد أكبر نسبياً لفهم مستوى الخطر .

وبالإضافة إلى سهولة القراءة فإن هناك ميزة لغوية أخرى قد تؤثر على مخاطر المراجعة وأتعاب المراجع وهي لغة التقاضي، فالكلمات القضائية هي كلمات تعكس الميل للمنافسة القانونية، وقد تم توثيق أن الكلمات القضائية مرتبطة بشكل كبير بالدعاوى القضائية، وتشير الكلمات الأكثر إثارة للتقاضي التي تستخدمها الشركات في إفصاحاتها عن الأمن السيبراني إلى وجود مخاطر أعلى للأمن السيبراني ضمنياً، وبالتالي فإن مخاطر الرقابة والمخاطر الكامنة المرتفعة تؤدي إلى بذل المراجع جهداً أكبر لتقليل مخاطر الاكتشاف.

وإنما يرى الباحثان أن أتعاب المراجعة تنظم السلوك المهني للمراجع وتعكس الجهد المبذول في عملية المصادقة بشكل أكثر دقة وحيادية، لتحسين جودة المعلومات الواردة في التقارير المالية، وعندما لا تستطيع أتعاب المراجعة تحمل هذه الجهد سيؤدى هذا إلى فشل آلية الإشراف على المراجع، وسيتحمل العميل أتعاب مراجعة غير عادية، فكلما ارتفعت مستوى المخاطر زادت أتعاب عملية المراجعة، حيث يقوم مراجع الحسابات بمزيد من الجهد لتخفيض هذه المخاطر ولهاذ تزداد الأتعاب بشكل غير طبيعي .

وحيث تعد أتعاب المراجعة دالة للجهد المطلوب للحصول على تأكيد معقول بأن البيانات المالية خالية من الأخطاء الجوهرية والأرباح العادية وأقساط مخاطر الرسوم الناشئة عن التقاضي المتعلق بعملية المراجعة، فإن هذه العوامل تشكل نموذج أتعاب المراجعة، ويتفق الباحثان مع دراسة Smith, T. J., et al. (2019) في أن نموذج الأتعاب يعكس جهد المراجع والمخاطر التي يتعرض لها في ضوء المتغيرات التكنولوجيا المعاصرة وبخاصة مخاطر اختراق الأمن السيبراني، وذلك على النحو التالي:

$$\mathbf{A(Audit\ Fees)=[cq+(E(d)\times E(r))]+[E(g)\times E(I)]+[E(t)\times E(z)]}$$

حيث :

-**[cq+(E(d)×E(r)]** : تمثل تكلفة عملية المراجعة للحصول على تأكيد معقول بأن البيانات المالية خالية من الأخطاء ، والأرباح العادية ، والخسائر التي يمكن أن تحدث إذا لم تكن البيانات المالية خالية من الأخطاء الجوهرية.

-**[E(g) × E(I)]** : تمثل التكاليف المرتبطة بالتقاضي المستقبلي المحتمل غير المرتبط بالتحريفات الجوهرية غير المكتشفة والتي يمكن أن يكون المراجع مسؤولاً عنها.

-**[E(t)× E(z)]** : هي التكاليف المستقبلية غير المتعلقة بالتقاضي (أي السمعة التالفة) من الارتباط بالبيانات المالية الحالية.

وعلى هذا يمكن توضيح أن شركات المراجعة تقيم المخاطر ليس فقط من خلال تقييم حوادث الاختراق السيبراني الفعلية ولكن أيضاً من خلال عمليات الإفصاح عن مخاطر الأمن السيبراني بشكل عام، حيث يدمج المراجع في تقييماته طبيعة ومحتوى الإفصاح عن مخاطر الأمن السيبراني وبالتالي يتأثر هيكل الأتعاب، ولذا يمكن للإفصاحات الأكثر إيضاحاً وقابلية للقراءة أن تخفض من أتعاب المراجعة وربما تكاليف المراقبة الأخرى التي تتحملها الشركات المقيدة في البورصة.

٢-٣-٢ ضعف الرقابة على التقارير المالية (ICFR) كأحد المسببات الناتجة عن مخاطر الأمن السيبراني

تمثل الرقابة الداخلية على التقارير المالية (ICFR) عملية مصممة من قبل أو تحت إشراف المسئولين التنفيذيين والماليين للشركة، أو الأشخاص الذين يؤدون وظائف مماثلة ويتم تنفيذها من قبل مجلس إدارة الشركة، والإدارة، والموظفين الآخرين لتقديم تأكيد معقول فيما يتعلق موثوقية التقارير المالية وإعداد البيانات المالية للأغراض الخارجية وفقاً لمبادئ المحاسبة المقبولة عموماً، وتتضمن ICFR أيضاً

الإجراءات والسياسات المتعلقة بمسك السجلات المحاسبية وتوثيق المعاملات وتفويض الإيصالات والنفقات وحماية الأصول، حيث تتطلب المادة ٤٠٤ من قانون Sarbanes-Oxley (SOX) من الإدارة تقييم فعالية ICFR الخاصة بشركتهم وتقديم تقرير عنها، ويتطلب أيضاً من المراجعين الخارجيين المصادقة والتقرير عن التقييمات التي أجرتها إدارة العميل، ومن ثم فإن المراجع الخارج مسئول قانوناً عن اكتشاف أوجه القصور في ICFR للشركات.

ونظراً لأن تأكيد الرقابة الداخلية على التقارير المالية ICFR يعد المسئولية المباشرة للمراجع الخارجي، فقد يُنظر إلى اختراق أحد العملاء على أنه فشل مراجعة في تقييم ICFR بشكل صحيح، مما قد يكون له آثار على العملاء الآخرين لمكتب المراجعة نفسه، وفى هذا السياق أوضح Joe, J. R. (2015) أن مجلس الرقابة على شركات المحاسبة العامة (PCAOB) يتطلب صراحةً من المراجعين الحصول على فهم لكيفية استخدام عملائهم لتكنولوجيا المعلومات (IT) وتأثير تكنولوجيا المعلومات في البيانات المالية، وبشكل أكثر تحديداً يتحمل المراجعون المسئولية عن اختبار ومراقبة ضوابط الوصول التي يقوم المراجعين بتنفيذها وتقييمها لتهديدات الأمن السيبراني في نموذج مخاطر المراجعة الخاص بهم، حيث تضمن مراجعة البيانات المالية ومراجعة ICFR الإجراءات المتعلقة بأنظمة التقارير المالية للشركة وتقييم مخاطر التحريف الجوهري الناتج عن الوصول غير المصرح به إلى هذه الأنظمة، وأوضحت دراسة Joe, J. R. (2015) أن المقابلات الشخصية التي تمت مع كبار مراجعي تكنولوجيا المعلومات في أكبر ٤ شركات مراجعة قدمت تأكيداً إضافياً حول أن مخاطر الأمن السيبراني أصبحت أكثر وأكثر أهمية كجزء من تقييم مخاطر المراجعة فعادةً ما يمثل مراجعة أنظمة تكنولوجيا المعلومات التي لا ترتبط ارتباطاً وثيقاً بالتقارير المالية مصدراً لأدلة مراجعة إضافية.

كما أشارت دراسة Haislip, J. Z., et al (2016) إلى أن استخدام تكنولوجيا المعلومات يؤثر في إعداد التقارير المالية على المراجعين الخارجيين، فبينما تعمل

تكنولوجيا المعلومات كأساس لضوابط داخلية أكثر فاعلية، فإنها تزيد أيضاً من تعرض الشركات للمخاطر المتعلقة بتكنولوجيا المعلومات، مثل مخاطر الأمن السيبراني، وربطت بعض الدراسات السابقة Lawrence, A., et al. (2018) بين حوادث الأمن السيبراني ونقاط الضعف المحتملة في الرقابة الداخلية حيث يمكن أن تتجسد مخاطر الأمن السيبراني في شكل ما يسمى بضعف الرقابة أكثر من التقرير (نقاط ضعف الرقابة في تكنولوجيا المعلومات)، أو كنقاط ضعف في "إعداد التقارير المالية" فقط.

وقد تشير حوادث الأمن السيبراني أيضاً إلى إخفاقات محتملة فيما يتعلق بالرقابة الداخلية على التقارير المالية، فالمراجع الخارجي مسئول قانوناً عن اكتشاف أوجه القصور في الرقابة الداخلية، ونظراً للاستخدام المتزايد لتكنولوجيا المعلومات في إعداد التقارير المالية وكذلك للأنشطة التجارية الأخرى، والطبيعة المترابطة المتزايدة لأنظمة تكنولوجيا المعلومات التجارية الحديثة على طول سلسلة القيمة، فإن المراجع مطالب عملياً بتوسيع عمليات المراجعة لتشمل أنظمة أخرى يمكن استغلالها من أجل الوصول غير المصرح به وذلك بغض النظر عن ما إذا كان النظام مرتبطاً بشكل مباشر بالتقارير المالية والمحاسبة، فحتى إذا لم يكن للهجمات الإلكترونية تأثير مباشر على أنظمة المحاسبة في الشركة، فقد يحتاج المراجع إلى بذل جهد إضافي لأن الهجمات الإلكترونية على طبقات الشبكة الداخلية أو المحيط قد تشير إلى نقاط ضعف في الضوابط العامة لتكنولوجيا المعلومات مما قد يشير إلى مخاطر في ICFR. Lawrence, A., et al. (2018)

وتوضح دراسة Rosati, P, et al. (2019) أن المراجع يزيد من أتعابه في العام السابق للإفصاح عن نقاط ضعف الرقابة الداخلية لتعكس الجهد الإضافي المطلوب لجمع أدلة مراجعة إضافية، ونظراً لأن حوادث الأمن السيبراني قد تشير إلى نقاط ضعف محتملة في الرقابة الداخلية، يكون من المتوقع أن نرى نمطاً مشابهاً في السنوات السابقة للحادث، على هذا النحو فإذا كان المراجع قادر على تقييم مخاطر

الأمن السيبراني للشركات العميلة بشكل صحيح، فيجب فرض أتعاب أعلى على العملاء الأكثر خطورة حتى قبل حدوث الاختراق.

كما يجادل بعض الممارسين بأنه يجب تحميل المراجعين المسئولية بعد وقوع حادث إلكتروني McKenna, F., (2019) وتوافقاً مع هذا الرأي أشارت دراسة Perols, R. R., Murthy, U. S. (2021) أن مراجع الحسابات قد يعانى من الإضرار بسمعته عندما يتم اختراق أحد عملائه، فقد يقوض حادث إلكتروني جودة المراجعة المتصورة والموقف التفاوضي لمكتب المراجعة الحالي Asthana, S. (2021) وفي ضوء ذلك فإن بذل جهود إضافية لمساعدة العملاء على تقليل مخاطر الأمن السيبراني يصب في مصلحة المراجعين.

كما تناقش دراسة Bao Ngo, T. N., & Tick, A. (2021) أن هناك العديد من الأسباب التي تدفع المنظمين وواضعي المعايير إلى إجبار مراجعي الحسابات على إعطاء المزيد من الاهتمام للشركات التي تقع في حوادث تتعلق بالأمن السيبراني **أولهما** تتمثل مهمة المراجع الخارجي في تقييم محاسبة العميل للخسائر والمطالبات والالتزامات المتعلقة بحوادث الأمن السيبراني بمجرد حدوثه في سياق شركة تجد صعوبة في التعامل مع التكلفة المباشرة وغير المباشرة الكبيرة وغير المتوقعة، **ثانيهما** في حالة وقوع هجمات إلكترونية مباشرة على نظام محاسبة الشركة ، فإن على المراجع مراعاة الرقابة الداخلية على إعداد التقارير المالية (ICFR) لأن الحادث قد يتضمن على مخاطر التلاعب في السجل المحاسبي للشركة، والذي ينتج عنه في البيانات المالية الأقل مصداقية، وحتى إذا لم تؤثر الهجمات الإلكترونية على نظام التسجيل المحاسبي، فلا يزال المراجع مطالب ببذل جهود إضافية في أعمال المراجعة الخاصة به نظراً لوجود مؤشرات حول نقاط الضعف في الرقابة الداخلية للشركة، والتي يمكن أن تكون مخاطر في ICFR، نظرًا لأن مراجعي الحسابات يتعرضون لضغوط هائلة عند مراجعة الشركات التي تتعرض لحوادث الأمن السيبراني، فمن الضروري أن تؤدى استجابتهم لحوادث الأمن السيبراني لزيادة أتعاب المراجعة.

وبناءً على المناقشة السابقة فإنه على المراجع الخارجي تقييم وفهم نقاط القوة والضعف في تكنولوجيا المعلومات الخاصة بالشركات بعناية ودمجها في تقييم المخاطر، وعلى ذلك فإنه يكون مسئول عن الحصول على فهم كاف للرقابة الداخلية على التقارير المالية من أجل تحديد وتقييم مخاطر التحريف الجوهري وتصميم وتنفيذ إجراءات مراجعة إضافية، ولذا من الممكن القول أن المراجع يفرض أتعاباً أعلى على العملاء الذين يعانون من أوجه قصور في الرقابة على التقارير المالية، وتستمر علاوة الأتعاب بعد عدة سنوات من إصلاح أوجه القصور.

وفي حالة وقوع حادث إلكتروني فمن المتوقع أن يأخذ المراجع في الاعتبار آثاره على ICFR، فإذا كان الهجوم مباشراً على أنظمة محاسبة الشركة فقد يشمل الحادث أو قد يشير إلى مخاطر التلاعب بدفاتر وسجلات الشركة، مما قد يؤثر على البيانات المالية، كما أنه نظراً لأن أنظمة المعلومات المحاسبية للشركات تلعب دوراً مركزياً في الأعمال ومن المحتمل أن تكون ثروة البيانات المخزنة على هذه الأنظمة ذات أهمية كبيرة، يجب على المراجع النظر في المخاطر المحتملة التي تأتي من تهديدات الأمن السيبراني، وبالنظر إلى أن المراجع يستجيب للمستويات الأعلى من مخاطر الرقابة من خلال توسيع إجراءات المراجعة الخاصة به وفرض أتعاب مراجعة أعلى، فمن المحتمل أن يتقاضى أتعاباً أعلى بعد وقوع حادث إلكتروني بناءً على تقييمه للمخاطر الرقابية.

٢-٣-٣ التحريفات الجوهرية في القوائم المالية للشركات التي تتعرض لضغوط الامتثال في ضوء الإفصاح عن مخاطر الأمن السيبراني

يخضع مراجع الحسابات لضغوط متزايدة من قبل المنظمين وواضعي المعايير فيما يتعلق بالأمن السيبراني، لذا يجب تركيز الضوء على حقيقة أنه يجب على المراجعين إعطاء اهتمام خاص لهذه الأنواع من الحوادث، وأن المراجع يمكن أن يلعب دوراً مهماً في منع أو التخفيف من آثار هذه الحوادث من خلال توفير ضمان إضافي حول ضوابط تكنولوجيا المعلومات الخاصة بعملائه، حيث يمثل الأمن

السيبراني خطراً متطوراً للمراجعين يتطلب تركيزاً مستمراً ، ويظل هذا الخطر حتى عندما لا يؤثر حادث سابق على الرقابة على التقارير المالية، لأنه قد يسلط الضوء على نقاط الضعف المحتملة، فحتى في حالة عدم تحديد حادثة إلكترونية معينة، يُطلب من المراجع أن يظل متشكك مهنياً طوال عملية المراجعة، لأن متوسط الوقت اللازم للتركيز على الحادث يزيد عن ستة أشهر، على وجه التحديد يجب على المراجع النظر في المخاطر المتعلقة بالأمن السيبراني التي يمكن أن تؤثر على مراجعة البيانات المالية، فإذا حدد المراجع المخاطر المتعلقة بالأمن السيبراني والتي يمكن أن يكون لها تأثيرات مادية على البيانات المالية لعملائهم يجب تصميم وتنفيذ إجراءات مصممة للتعامل مع المخاطر المعينة. (Rosati, P, et al (2019

وبشكل عام تقوم شركات المراجعة بتعديل أساليب أو إجراءات المراجعة الخاصة بها لمعالجة التأثير المحتمل للحوادث الإلكترونية على الضوابط ذات الصلة في عمليات المراجعة اللاحقة، كما أنشأت بعض شركات المراجعة مجموعة من خبراء الأمن السيبراني لمعالجة مخاطر الأمن السيبراني، ولهذا يمكن القول إن الوقت والجهد المبذولين من قبل مكتب المراجع لفهم محددات وعواقب الحوادث السيبرانية لهما قيمة كبيرة لعملائه الآخرين أيضاً، حيث يستخدم المتسللون عادةً نفس الأساليب أو أساليب مشابهه لاستهداف شركات مختلفة.

واستناداً لما سبق فإن المراجع الخارجي قد يعدل ممارساته بناءً على تجارب الأمن السيبراني السابقة ويبذل المزيد من جهد المراجعة لمعالجة مشكلات الأمن السيبراني لعملائه غير المخترقين، وستؤدي هذه الجهود أو الإجراءات الإضافية إلى زيادة أتعاب المراجعة، ويمكن القول أيضاً أن أتعاب المراجعة لا يتم تحديدها من قبل المراجعين فقط، ولكنها تعكس مفاوضات بين الإدارة والمراجع. وفي الواقع تشير الأدلة إلى أن المراجع قد يجد صعوبة في رفع الأتعاب بسبب المنافسة الشديدة مع العملاء الجدد (Richardson, V., et al(2019، ومع ذلك نظراً لأن هيئة البورصة الأمريكية (SEC) أكدت على الأمن السيبراني فإن الشركات تتعرض

لضغوط الامتثال لتوجيهات الإفصاح عن الأمن السيبراني منها وتطلب المساعدة بشكل عاجل في تقييم ضوابط الأمن السيبراني، ونظراً لأن المراجعين أكثر قدرة على تحديد مشكلات الرقابة من المديرين، فإن خبرتهم قد تساعد المديرين على تحسين استعداد الشركات للهجمات الإلكترونية Li, H., et al. (2020) ، ومن ثم فمن المفهوم أن علاوة أتعاب تجربة الأمن السيبراني ستكون مقبولة للمديرين.

وفى هذا السياق يمكن أن تؤثر مخاطر الأمن السيبراني بشكل جوهري على أتعاب المراجعة حيث يمكن أن تؤدي المخاطر المرتفعة إلى مزيد من التخطيط والاختبار للمراجعة للتحقق من عدم المساس بالضوابط الداخلية على التقارير المالية، فقد يؤدي نظام الرقابة الداخلية المخترق إلى احتمالية أكبر للتحريف الجوهري إما بسبب الأخطاء أو الاحتيال، بالإضافة إلى ذلك يمكن أن يكون للتهديدات التي يتعرض لها الأمن السيبراني آثار كبيرة على فعالية الرقابة الداخلية في المستقبل، وبالتالي قد يكون المراجع ملزماً بالتحقيق فيما إذا كانت الإدارة قد نفذت ضوابط مناسبة بعد تهديد معروف وما إذا كانت الضوابط التي تم تنفيذها ستقلل من مخاطر التحريفات الجوهرية المستقبلية في البيانات المالية للعميل، و في هذا السياق أشار Hamm, K. (2019) إلي أنه:

إذا حدد المراجع خطراً متعلقاً بالأمن السيبراني يمكن أن يكون له تأثير مادي على البيانات المالية للشركة، فيجب على المراجع بعد ذلك تصميم وتنفيذ الإجراءات لمعالجة تلك المخاطر، بالنسبة للمراجعة المتكاملة، قد يشمل هذا العمل اختبار الضوابط ذات الصلة.

كما أوضحت دراسة Hamm, K. (2019) أنه سواء وقعت حادثة إلكترونية أم لا أثناء عملية التخطيط، فإنه يجب على المراجع إجراء تقييم للمخاطر، ويجب أن يأخذ هذا التقييم في الاعتبار أي مخاطر للأمن السيبراني يمكن أن لها تأثير جوهري على البيانات المالية للشركة، لذلك فمن المعقول للغاية أن تزيد أتعاب المراجعة استجابةً لمخاطر الأمن السيبراني للعميل والطريقة التي يتم بها معالجة هذه المخاطر والإفصاح عنها،

كما يجب أن يحصل المراجعون على فهم شامل لمخاطر العمل التي يواجهها العميل من المصادر المهمة المحتملة للمعلومات حول المخاطر عمليات الإفصاح عن مخاطر الأعمال والمعلومات التي يقوم بها العميل في التقارير العامة. ويمكن أن تكون مخاطر الأمن السيبراني، وهي عنصر أساسي في الإفصاح عن المخاطر من قبل منتشرة وتؤثر على سلامة نظام المعلومات المالية بالكامل، أو محددة وتؤثر فقط على التطبيقات الفردية أو قطاعات البيانات في نظام المعلومات المالية.

وقد ترتبط الحوادث السيبرانية أيضاً بمخاطر التحريف الجوهري، فقد يؤدي وقوع الحوادث الإلكترونية إلى زيادة مخاطر الأعمال التجارية للعميل، والتي تشير إلى "خطر تدهور الوضع الاقتصادي للعميل على المدى القصير أو الطويل"، وتشير دراسة M. Mazboudi. (2016)&Khalil, S., إلى أن المراجعين الخارجيين يقيّمون مخاطر أعمال العميل عند تحديد ما إذا كانوا سيقبلون عميلاً جديداً، ويقل احتمال قبولهم لممارسة المحاسبة المقترحة من قبل العميل إذا كانت مخاطر عمل العميل عالية.

وسواء كانت مخاطر الأمن السيبراني منتشرة أو محددة، فمن المحتمل أن يكون لها تأثير على فعالية كل من الضوابط العامة وضوابط التطبيق في سياق نظام التقارير المالية، وتؤثر هذه المخاطر بدورها على فعالية نظام الرقابة الداخلية للشركة، وبالتالي تزيد من احتمالية وجود أخطاء جوهرية في البيانات المالية إما بسبب أخطاء أو احتيال Smith, T. J., et al. (2019)، حيث يتطلب معيار المراجعة المصري والدولي رقم (٣١٥) بعنوان "تحديد مخاطر التحريف الجوهري وتقييمها من خلال فهم المنشأة وبيئتها" على ضرورة أن يحدد المراجع مخاطر التحريف الجوهري وتقييمها سواء كانت بسبب غش أو خطأ، على مستوى القوائم المالية ومستوى الإقرارات، وذلك من خلال فهم المنشأة وبيئتها بما في ذلك الرقابة الداخلية للمنشأة، ومن ثم توفير أساس لتصميم وتنفيذ استجابات لمخاطر التحريف الجوهري المقيمة، كما يتطلب قانون

Sarbanes-Oxley لعام ٢٠٠٢ من مراجعي الشركات المملوكة ملكية عامة مراجعة ضوابط وإجراءات العملاء لتشهد على تقييم الإدارة للضوابط الداخلية.

وفقاً لذلك عندما يعتقد المراجع أن العميل يواجه مستوى مرتفعاً من مخاطر الأمن السيبراني، فقد يقوم بتعديل تقديرات المخاطر الكامنة (IR)، أو مخاطر الرقابة (CR)، أو مخاطر الاكتشاف (DR) في التخطيط لعملية المراجعة وإجرائها، وتحدد طبيعة عمل العميل ونظام الرقابة الداخلية مستوى المخاطر الكامنة ومخاطر الأمن السيبراني، ولكن يحتاج المراجع إلى إدارة مخاطر الاكتشاف من أجل ضمان مستوى مقبول من المخاطر الإجمالية لإبداء رأي مناسب حول البيانات المالية للعميل، على وجه الخصوص يتطلب المستوى المرتفع للمخاطر الكامنة أو مخاطر الأمن السيبراني من المراجع خفض معدل الاسترداد من أجل تحقيق مستوى مناسب من مخاطر المراجعة الشاملة.

ولهذا أشارت دراسة Calderon, T. G., & Gao, L. (2021) إلى أنه مع زيادة المخاطر الكامنة وسجلات العملاء بسبب مشكلات الأمن السيبراني، يخفض المراجع من مخاطر الاكتشاف عن طريق إجراء اختبارات أكثر تفصيلاً، مما يؤدي عموماً إلى زيادة أتعاب المراجعة، إضافة إلى أنه نظراً للطبيعة السرية للتهديدات السيبرانية والتأثير المنتشر المحتمل على نظام المعلومات المالية، فمن المتوقع أنه حتى مع مستوى أعلى من اختبار المراجعة لن يكتشف الأخطاء الجوهرية التي تحركها قضايا الأمن السيبراني.

ونظراً لأن المراجع قد يقيّم مستويات أعلى من المخاطر الكامنة ومخاطر الأمن السيبراني للعميل الذي يعاني من مخاطر عالية للأمن السيبراني، فمن المحتمل أن يقوم المراجع أيضاً بتعيين علاوة على أتعاب المراجعة لتقييم فئة المخاطر المتزايدة التي قد يقع فيها العميل، بالإضافة إلى الآثار العكسية المحتملة للتهديدات السيبرانية الخفية لمحاولة الحد من هذه الآثار مخاطر خلال اختبارات إضافية، وبالتالي يمكن تعديل

نموذج أتعاب المراجعة ليأخذ في الحسبان العمل الإضافي الذي يجب على المراجع القيام به بسبب المخاطر الكامنة العالية ومخاطر الأمن السيبراني بالإضافة إلى أتعاب المخاطر التي قد يفرضها المراجع على عميل في فئة مخاطر أعلى بشكل عام.

بينما تجادل المناقشة السابقة بأن المراجع سيزيد أتعابه بعد وقوع الحوادث السيبرانية كاستراتيجية استجابة، فإنه لا يزال من غير الواضح ما إذا كان المراجعون الخارجيون يسعون إلى فحص مخاطر الأمن السيبراني الجوهرية قبل وقوع الحوادث السيبرانية، حيث يشير نموذج أتعاب المراجعة إلى أن الأتعاب ستعكس التكاليف التي تنشأ من مخاطر عدم التقاضي مثل خسارة العميل، وأن المراجعين الخارجيين يحددون أي تكلفة متوقعة ناتجة عن الخسائر المحتملة مثل الدعاوى القضائية المستقبلية أو الإضرار بالسمعة. ونظراً لأن مخاطر الأمن السيبراني لها آثار على الأداء المستقبلي للشركة، وعلاقات العملاء، وبيئة الرقابة فمن المتوقع أن يقوم المراجعون الخارجيون بدمج مخاطر الأمن السيبراني المادية في أتعاب المراجعة حتى قبل وقوع الحوادث الإلكترونية.(Yang, L., et al. (2020

وبالنظر إلى المناقشة السابقة يتبين للباحثان بوضوح أن انتهاكات الأمن السيبراني بغض النظر عن طبيعتها لها آثار محتملة على المراجع الخارجي وأنه مطالب أيضاً بتقييم مخاطر عملائه المتعلقة بالأمن السيبراني بغض النظر عن ما إذا كانوا قد تأثروا بالفعل بالاختراق، ولذلك يجب تضمين مخاطر الأمن السيبراني في تقييم مخاطر تكنولوجيا المعلومات للعملاء، وعلى هذا النحو يجب أن تكون جزءاً من التقييم الشامل لمخاطر المراجعة، لذا يبذل المراجع جهداً إضافياً من أجل تقييم الآثار المترتبة وبالتالي التخفيف من زيادة مخاطر المراجعة، ونتيجة للجهود الإضافية فمن المتوقع أن توجد زيادة في أتعاب المراجعة.

وبناءً على ما تم عرضه فإنه يمكن اشتقاق الفروض البحثية تمهيداً لاختبارها على النحو التالي في ضوء الدراسة التطبيقية:

الفرض الإحصائي الأول: *لا يوجد تأثير ذو دلالة إحصائية للإفصاح عن مخاطر الأمن السيبراني باستخدام أسلوب تحليل المحتوى على أتعاب عملية المراجعة.*

الفرض الإحصائي الثاني: *لا يوجد تأثير ذو دلالة إحصائية لتعرض الشركة للهجمات السيبرانية على أتعاب عملية المراجعة.*

القسم الثالث: تصميم الدراسة التطبيقية واختبار الفروض البحثية:

هدفت الدراسة الحالية إلي التعرف على دور الإفصاح عن مخاطر الأمن السيبراني في التأثير على أتعاب عملية المراجعة، ونظراً لأن البيئة المصرية للشركات المقيدة في سوق الأوراق المالية تعاني من ضعف شديد في الإفصاح عن العمليات التكنولوجية الموجودة بها فضلاً عن رفض غالبية الشركات التوجه نحو استخدام التقنيات التكنولوجية المستحدثة، وقد يكون السبب الرئيسي لذلك هو ضعف البنية التحتية وضخامة الاستثمارات اللازمة لذلك فضلاً عن مقاومة البيئة التي تعمل بها الشركة لتلك التطورات لما لها من آثار سلبية على الروتين اليومي للعاملين بتلك الشركات وحجم العمالة أيضاً. وبالتالي، تتسم البيئة المحاسبية المصرية بضعف البنية التكنولوجية بشكل عام وضعف الرقابة على التقنيات الرقمية بشكل خاص.

ولغرض اختبار فروض الدراسة فإنه يجب أولاً تحديد البيانات الأكثر ملاءمة مع طبيعة البيئة التكنولوجية للشركات المقيدة في سوق الأوراق المالية المصري، وبالتالي سيقوم الباحثان بتخصيص هذا الجزء من الدراسة لعرض الإجراءات التي يجب القيام بها لاختبار الفروض الإحصائية، والنتائج التي تم التوصل إليها من تحليل البيانات وتشغيل نموذج اختبار الفروض، والتفسير الممكن لتلك النتائج وذلك على النحو التالي:

٣-١: صياغة الفروض الإحصائية للدراسة:

أضفت الرؤية المصرية ٢٠٣٠ نحو التحول الرقمي المزيد من المسئوليات على عاتق المسئولين والمنظمين لمهنة المحاسبة والمراجعة، حيث تدفع هذه الرؤية الشركات دفعاً نحو التحول الرقمي والابتعاد عن الأساليب التقليدية، ومن ثم تطور مسئوليات المحاسبة والمراجعة، وعلى الرغم من الاهتمام بتحقيق تلك الرؤية في البيئة المصرية، إلا أن الشركات المتحولة رقمياً تتسم بالندرة الشديدة فضلاً عن عدم اهتمام هيئة سوق المال بتحقيق التطور الإلزامي للإفصاح عن تلك الممارسات الرقمية، ومن هذا المنطلق يمكن للباحثان صياغة الفروض الإحصائية للدراسة بما يتفق مع البيئة الضعيفة للتقنيات الرقمية المصرية.

ولذلك فإن الإفصاح عن الأمن السيبراني يكاد يكون غير موجود في البيئة المصرية للشركات المدرجة في سوق المال، ومن ثم سيلجأ الباحثان إلي استخدام تحليل المحتوى للتقارير السردية من مجالس الإدارة واجتماعات الجمعية العمومية للتطرق إلي أية إشارة عن الأمن السيبراني في تلك التقارير. وبالتالي، يمكن صياغة الفرض الإحصائي الأول للدراسة على النحو التالي:

الفرض الإحصائي الأول للدراسة: لا يوجد تأثير ذو دلالة إحصائية للإفصاح عن مخاطر الأمن السيبراني باستخدام أسلوب تحليل المحتوى على أتعاب عملية المراجعة.

كما يندر أو ينعدم الإفصاح عن تعرض تلك الشركات المقيدة في سوق الأوراق المالية المصري للهجمات السيبرانية وذلك حفاظاً على سمعة الشركة أمام الأطراف الخارجية ذوي المصلحة. وعلى الرغم من ذلك، سيقوم الباحثان باستغلال هذه الهجمات السيبرانية كأحد الدلالات على أهمية الإفصاح عن مخاطر الأمن السيبراني وذلك من خلال تتبع تلك الهجمات من الصحف أو المواقع الالكترونية أو الأخبار على الموقع الالكتروني للشركة نفسها، وهو ما قد يزيد من حجم المسئولية على عاتق المراجع الخارجي ومن ثم توقع زيادة الأتعاب، وعليه يمكن صياغة الفرض الإحصائي الثاني للدراسة على النحو التالي:

الفرض الإحصائي الثاني للدراسة: *لا يوجد تأثير ذو دلالة إحصائية لتعرض الشركة للهجمات السيبرانية على أتعاب عملية المراجعة.*

٣-٢: توصيف متغيرات الدراسة وأدوات القياس:

استناداً إلي العرض السابق للإطار النظري لصياغة الفروض الإحصائية للدراسة يمكن للباحثان عرض متغيرات الدراسة وأدوات قياسها لأغراض تحليل العلاقة بين المتغيرات على النحو التالي:

٣-٢-١: المتغير المستقل للدراسة:

تتمثل المتغيرات المستقلة محل الاهتمام في الدراسة الحالية في كل ما يتعلق بالإفصاح عن الأمن السيبراني من إفصاحات سردية أو كمية أو حتى نوعية. وعليه تختص الإفصاحات السردية بكافة تقارير مجالس الإدارة والاجتماعات للجمعية العمومية فيما يتعلق بأي شئ يخص الأمن السيبراني على أن يتم تحليل محتواه، بينما يتعلق الإفصاح الكمي عن أدوات التأمين ضد مخاطر الأمن السيبراني فيما يتم دفعه من استثمارات للتأمين ضد مخاطر الأمن السيبراني، أما الإفصاحات النوعية فهي الإفصاحات عن أي هجمات سيبرانية من خلال الأخبار ومواقع الإنترنت سواء تخص الشركة أو لا تخصها، وبالتالي يمكن للباحثان تقسيم الإفصاحات عن مخاطر الأمن السيبراني في ضوء أسلوب تحليل المحتوى على النحو التالي:

١- الإفصاحات السردية عن مخاطر الأمن السيبراني:

تمثل الإفصاحات السردية عن مخاطر الأمن السيبراني الجزء الأهم من مخاطر الإفصاح عن الأمن السيبراني وعليه يمكن استخدام أسلوب تحليل المحتوى من خلال حصر الكلمات الدالة على تهديد الأمن السيبراني والكلمات الدالة على احتمالية التقاضي بسبب مخاطر الأمن السيبراني، ولذلك يمكن قياس مستوى الإفصاح السردي عن مخاطر الأمن السيبراني باتباع طريقة تحليل المحتوى، ويتم استبعاد المشاهدات التي لم تقم فيها الشركة بالإفصاح عن أية مخاطر للأمن السيبراني.

وفي النهاية تسفر حصيلة الكلمات عن المقياسين التاليين لتحليل المحتوى للإفصاح عن مخاطر الأمن السيبراني:

- لوغاريتم عدد الكلمات الدالة على الإفصاح عن مخاطر الأمن السيبراني.
- لوغاريتم عدد الكلمات الدالة على التقاضي فيما يتعلق بالأمن السيبراني ومخاطر تكنولوجيات المعلومات.

٢- الإفصاحات الكمية عن مخاطر الأمن السيبراني:

يتمثل هذا النوع من الإفصاح عن مخاطر الأمن السيبراني في المبالغ التي يتم دفعها للاستثمار في الأصول التي تساهم في التأمين ضد مخاطر الأمن السيبراني، ولذلك يمكن الاستناد إلي رقم قيمة استثمارات تكنولوجيا المعلومات والتأمين ضد مخاطرها الموجود بالأصول الثابتة أو في بند مشروعات تحت التنفيذ.

٣- الإفصاحات النوعية عن الهجمات السيبرانية:

يتسم هذا النوع من الإفصاحات بالندرة الشديدة بل ويصل إلي حد الإنعدام في بعض الأحيان ويمكن قياسه باستخدام متغير وهمي يأخذ القيمة ١ في حالة وجود ما يدل على حدوث هجمات سيبرانية من خلال تتبع مواقع الأخبار عن الشركة وكذلك الموقع الالكتروني للشركة نفسه والقيمة صفر فيما عدا ذلك.

٣-٢-٢: المتغير التابع للدراسة:

ونظراً لأنه في البيئة المصرية يتم تحديد واعتماد أتعاب المراجعين مقدماً وبشكل سنوي خلال اجتماع الجمعية العامة العادية للمساهمين والذي يعقد خلال الأشهر الأولى من السنة المالية للعميل، فإن هذا يعني أن أتعاب عملية المراجعة التي تم الاتفاق عليها بين المراجع والعميل والتي تم عرضها على الجمعية العامة العادية لاعتمادها يكون قد تم تقديرها بناءً على ما انتهت إليه، ومن ثم يمثل الرقم المتفق عليه هو مقياس أتعاب المراجعة الكلي.

ويمكن أيضاً الحصول على الأتعاب غير العادية لعملية المراجعة باستخدام نموذج أتعاب عملية المراجعة كما ورد في الدراسات السابقة Bao Ngo, T. N., & Tick, A. (2021); Li, H., No, W. G., & Boritz, J. E. (2020); Smith, T. J., et al (2019); Rosati, P., Gogolin, F., & Lynn, T. (2019) والملائم لسوق خدمات المراجعة في البيئة المصرية حالياً والمطور من قبل الباحث لقياس الأتعاب غير العادية لعملية المراجعة، ويأخذ ذلك النموذج الشكل التالي:

$$LnAF_{it} = \beta0 + \beta1\ (LnTA_{it}) + \beta2\ (SQSUB_{it}) + \beta3\ (FOREIGN_{it}) + \beta4\ (LnSEG_{it}) + \beta5\ (RECINV_{it}) + \beta6\ (QUICK_{it}) + \beta7\ (LEV_{it}) + \beta8\ (ROA_{it}) + \beta9\ (LOSS_{it,t-1,t-2}) + \beta10\ (SGROWTH_{it}) + \beta11\ (MTB_{it}) + \beta12\ (SPEC_{it}) + \beta13\ (INITIAL_{it}) + \beta14\ (LnARLAG_{it}) + \beta15\ (YEND_{it}) + \text{industry and year dummies} + \varepsilon_{it} \quad (1)$$

حيث إنه بالنسبة للشركة I في السنة t أو في السنة t-1(أي السنة السابقة) أو في السنةt-2 (أي السنة قبل السابقة)، فإن:

LnAF = اللوغاريتم الطبيعي للأتعاب الفعلية المدفوعة للمراجع الخارجي مقابل عملية المراجعة؛

LnTA = اللوغاريتم الطبيعي لإجمالي الأصول؛

SQSUB = الجذر التربيعي لعدد الشركات التابعة التي تشملها القوائم المالية المجمعة؛

FOREIGN = نسبة عدد الشركات التابعة الخارجية إلي إجمالي عدد الشركات التابعة؛

LnSEG = اللوغاريتم الطبيعي لعدد قطاعات الأنشطة؛

RECINV = نسبة مجموع المخزون والعملاء وأوراق القبض إلي إجمالي الأصول؛

QUICK = نسبة التداول السريع (وتقاس بنسبة الأصول المتداولة باستبعاد المخزون إلي الالتزامات المتداولة)؛

LEV = نسبة الرافعة المالية (وتقاس بنسبة الالتزامات طويلة الأجل أو إجمالي الالتزامات إلي إجمالي الأصول أو إجمالي حقوق الملكية)؛

ROA = العائد على الأصول (و يقاس بنسبة صافي الدخل قبل الضرائب إلي إجمالي الأصول؛

LOSS = متغير وهمي، بحيث يأخذ القيمة ١ في حالة تكبد صافي خسارة، بينما يأخذ القيمة ٠ فيما عدا ذلك؛

SGROWTH = معدل نمو المبيعات السنوي؛

MTB = نسبة القيمة السوقية إلي القيمة الدفترية للسهم؛

SPEC = متغير وهمي، بحيث يأخذ القيمة ١ في حالة بلوغ مكتب المراجعة نسبة معينة للحصة السوقية لصناعة معينة أو زاد عليها، بينما يأخذ القيمة ٠ فيما عدا ذلك – أو متغير مستمر بحيث يأخذ النسبة الفعلية الناتجة من معادلة حساب الحصة السوقية لمكتب المراجعة في حصة معينة؛

INITIAL = متغير وهمي، بحيث يأخذ القيمة ١ في حالة السنة الأولى للتعاقد بين المراجع الخارجي والعميل، بينما يأخذ القيمة ٠ فيما عدا ذلك؛

LnARLAG = اللوغاريتم الطبيعي لعدد الأيام المنقضية من تاريخ نهاية السنة المالية وحتى تاريخ إصدار تقرير المراجعة؛

YEND = متغير وهمي، بحيث يأخذ القيمة ١ في حالة انتهاء السنة المالية خلال موسم الذروة بالنسبة للمراجعين الخارجيين، بينما يأخذ القيمة ٠ فيما عدا ذلك؛

$\beta 0, \beta 1, \beta 2 \ldots \beta K$ = معلمات الانحدار؛

ε = بواقي النموذج، والتي تستخدم كمقياس للأتعاب غير العادية لعملية المراجعة.

ونظراً لأنه في البيئة المصرية يتم تحديد واعتماد أتعاب المراجعين مقدماً وبشكل سنوي خلال اجتماع الجمعية العامة العادية للمساهمين والذي يعقد خلال الأشهر الأولى من السنة المالية للعميل، فإن هذا يعني أن أتعاب عملية المراجعة التي تم الاتفاق عليها بين المراجع والعميل والتي تم عرضها على الجمعية العامة العادية لاعتمادها يكون قد تم تقديرها بناءً على ما انتهت إليه أعمال السنة السابقة، وبالتالي فمن المنطقي القول أن المتغيرات التفسيرية الواردة بالنموذج السابق يجب أن يتم التعويض عنها بقيمتها طبقًا للمعلومات الخاصة بالسنة السابقة، وذلك فيما عدا المتغير YEND، حيث تكون تلك المتغيرات معلومة بالفعل مقدماً لحظة تقدير الأتعاب من قبل المراجع والتفاوض بشأنها مع العميل دون الحاجة للانتظار حتى نهاية السنة المالية للعميل.

هذا وسيتم تشغيل النموذج السابق باستخدام كافة الشركات المتاح عنها البيانات اللازمة لتشغيله، مع تجميع كافة الشركات المتاحة في كل سنة خلال فترة الدراسة في مجموعة بيانات واحدة وتشغيل النموذج عليها بالكامل (Pooled Regression)، وبعد أن يتم تشغيل النموذج بالكيفية السابقة، فإن الباحثان سيستخدمان البواقي التي تحمل إشارة موجبة وسالبة كمقياس للأتعاب غير العادية لعملية المراجعة، حيث تمثل تلك البواقي الفرق بين الأتعاب الفعلية المدفوعة للمراجع الخارجي والأتعاب العادية المقدرة من قبل النموذج، وتلك البواقي التي تحمل إشارة

موجبة تعكس تسعير خدمات المراجعة بأكبر مما يجب (أتعاب غير عادية موجبة). بينما تعكس البواقي التي تحمل إشارة سالبة تسعير خدمات المراجعة بأقل مما يجب (أتعاب غير عادية سالبة).

٣-٢-٣: المتغيرات الضابطة للعلاقة:

تتمثل أهم المتغيرات الضابطة للعلاقة في المتغيرات الخاصة بالتأثير على المتغير التابع للدراسة والخاصة بأتعاب عملية المراجعة، والتي يتمثل أهمها من وجهة نظر الباحثان في:

المتغير	الرمز	التفسير
إجمالي الأصول	LNTA	لوغاريتم القيمة الدفترية لإجمالي الأصول
الرافعة المالية	LEV	إجمالي الالتزامات مقسومة على إجمالي الأصول
معدل العائد على الأصول	ROA	صافي الدخل مقسوماً على إجمالي الأصول
مؤشر الخسارة	LOSS	متغير وهمي يأخذ القيمة ١ في حالة الخسارة والقيمة صفر فيما عدا ذلك
المراجعين الكبار	BIG 4	متغير وهمي يأخذ القيمة ١ اذا كان المراجع من الشركات العالمية والقيمة صفر فيما عدا ذلك

٣-٣: نموذج تحليل العلاقة بين متغيرات الدراسة.

في إطار تحليل متغيرات الدراسة وصياغة الفروض الإحصائية يمكن للباحثان صياغة نموذج الدراسة من خلال العرض التالي:

٣-٣-١: نموذج اختبار الفرض الإحصائي الأول للدراسة:

يتنبأ الفرض الأول للدراسة بتحليل أثر الإفصاح عن مخاطر الأمن السيبراني باستخدام أسلوب تحليل المحتوى على أتعاب عملية المراجعة. ومن ثم يمكن للباحثان صياغة النموذج الإحصائي لاختبار الفرض الأول على النحو التالي:

$$Ln\ AF = \beta0 + \beta1\ LnWords + \beta2\ LITIGIOUS + \beta3\ LNTA + \beta4\ LEV + \beta5\ ROA + \beta6\ LOSS + \beta7\ BIG4 + \varepsilon_{it} \quad (2)$$

$$PABAF = \beta0 + \beta1\ LnWords + \beta2\ LITIGIOUS + \beta3\ LNTA + \beta4\ LEV + \beta5\ ROA + \beta6\ LOSS + \beta7\ BIG4 + \varepsilon_{it} \quad (3)$$

$$NABAF = \beta0 + \beta1\ LnWords + \beta2\ LITIGIOUS + \beta3\ LNTA + \beta4\ LEV + \beta5\ ROA + \beta6\ LOSS + \beta7\ BIG4 + \varepsilon_{it} \quad (4)$$

حيث أن:

LnWords = لوغاريتم عدد الكلمات الدالة على الإفصاح عن مخاطر الأمن السيبراني؛

LITIGIOUS = لوغاريتم عدد الكلمات الدالة على التقاضي فيما يتعلق بالأمن السيبراني ومخاطر تكنولوجيات المعلومات؛

Ln AF = اللوغاريتم الطبيعي لإجمالي أتعاب عملية المراجعة التي تم تقاضيها؛

PABAF = بواقي النموذج رقم (١) الموجبة والمعبرة عن الأتعاب غير العادية الموجبة؛

NABAF = بواقي النموذج رقم (١) الموجبة والمعبرة عن الأتعاب غير العادية السالبة؛

٣-٣-٢: نموذج اختبار الفرض الإحصائي الثاني للدراسة:

يتنبأ الفرض الثاني للدراسة بتحليل أثر الهجمات السيبرانية على أتعاب عملية المراجعة، ومن ثم يمكن للباحثان صياغة النموذج الإحصائي لاختبار الفرض الثاني على النحو التالي:

$$Ln\ AF = \beta_0 + \beta_1\ CI + \beta_2\ LNTA + \beta_3\ LEV + \beta_4\ ROA + \beta_5\ LOSS + \beta_6\ BIG4 + \varepsilon_{it} \quad (5)$$

$$PABAF = \beta_0 + \beta_1\ CI + \beta_2\ LNTA + \beta_3\ LEV + \beta_4\ ROA + \beta_5\ LOSS + \beta_6\ BIG4 + \varepsilon_{it} \quad (6)$$

$$NABAF = \beta_0 + \beta_1\ CI + \beta_2\ LNTA + \beta_3\ LEV + \beta_4\ ROA + \beta_5\ LOSS + \beta_6\ BIG4 + \varepsilon_{it} \quad (7)$$

حيث أن:

CI = متغير وهمي يأخذ القيمة ١ في حالة وجود ما يدل على حدوث هجمات سيبرانية من خلال تتبع مواقع الأخبار عن الشركة وكذلك الموقع الالكتروني للشركة نفسه والقيمة صفر فيما عدا ذلك.

٣-٤: مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في الشركات المقيدة في البورصة المصرية والمتاحة للتحميل على الموقع الإلكتروني للبورصة المصرية، وتمثلت عينة الدراسة في عدد من هذه الشركات والتي يتوافر فيها بيانات قياس المتغيرات وعددها (١٥) شركة بواقع ٧٥ مشاهده، حيث تمثلت هذه المشاهدات في القوائم المالية للشركات عينة الدراسة خلال الفترة من ٢٠١٧ حتى ٢٠٢١، وتقارير الحوكمة، وتقرير هيكل المساهمين وهيكل مجلس الإدارة ومحاضر اجتماعات لجان المراجعة ومحاضر اجتماع الجمعية العمومية.

وقام الباحثان باستبعاد المؤسسات المالية (مثل البنوك، شركات التامين،) من عينة الدراسة، وذلك لما تتسم به تلك المؤسسات من خصائص تشغيلية تختلف اختلافا جوهريا عن بقية الشركات، الأمر الذي يجعل قيم بعض المتغيرات الضابطة لها بالإضافة إلي خضوعها لقوانين وقواعد تنظيمية خاصة بها، ويشير الجدول التالي إلي الشركات عينة الدراسة على النحو التالي:

م	أسماء الشركات	م	أسماء الشركات
١	كفر الزيات للمبيدات والكيماويات	٩	أبو قير للأسمدة والصناعات الكيماوية
٢	أوراسكم	١٠	الشركة الدولية للمحاصيل الزراعية
٣	شركة الصعيد العامة للمقاولات والاستثمار العقارى	١١	شركة الإسكندرية للغزل والنسيج
٤	إم إم جروب للصناعة والتجارة العالمية	١٢	الشرقية الوطنية للأمن الغذائي
٥	الدولية للصناعات الطبية ايكمي	١٣	مصر للزيوت والصابون
٦	شركة الكابلات الكهربائية المصرية	١٤	الدلتا للسكر
٧	شركة شارم دريمز	١٥	أسمنت قنا
٨	النساجون الشرقيون		

ويرجع السبب في اختيار تلك الشركات للأسباب التالية:

- توافر محاضر الجمعيات العامة العادية للشركات ابتداءً من عام ٢٠١٧ حتى عام ٢٠٢١.
- توافر البيانات الخاصة بالحوكمة والمتمثلة في نمط هيكل الملكية وخصائص مجلس الإدارة وخصائص لجنة المراجعة.
- توافر تقرير الإفصاح عن هيكل المساهمين وهيكل مجلس الإدارة وتقارير الحوكمة ولجان المراجعة ابتداءً من عام ٢٠١٧ حتى عام ٢٠٢١.

٣-٥: نتائج الدراسة:

يمكن للباحثان استعراض نتائج الدراسة من خلال ثلاثة محاور أساسية يتمثل الأول في عرض الإحصاءات الوصفية للمتغيرات المستخدمة في الدراسة، ويتمثل الثاني في عرض مصفوفة ارتباط بيرسون بين متغيرات الدراسة، ويتمثل الثالث في عرض نتائج اختبارات الفروض الإحصائية للدراسة. ولكن قبل استعراض نتائج الدراسة يصبح من الأهمية بمكان تشغيل نموذج الأتعاب لتحديد المشاهدات التي تعبر عن الأتعاب غير العادية الموجبة والسالبة وهي محل اهتمام الدراسة، وذلك على النحو التالي:

٣-٥-١: تشغيل نموذج الأتعاب:

من خلال تشغيل نموذج الأتعاب في البيئة المصرية على المشاهدات المدرجة بعينة الدراسة تبين للباحثان ارتفاع القوة التفسيرية للنموذج المطبق حيث بلغت ٥٩,٩% أي أن المتغيرات المدرجة بالنموذج قادرة على تفسير ٥٩,٩% من التغير في الأتعاب لعملية المراجعة وهو ما يتضح من نتائج الجدول رقم (١)، وهي نسبة جيدة اذا ما قورنت بنظائرها في الدراسات السابقة ذات الصلة.

بالإضافة إلي ذلك تبين للباحثان من تشغيل النموذج أن البواقي المستخرجة تنقسم إلي عدد ٣٩ مشاهدة خاصة بالأتعاب غير العادية الموجبة (أتعاب مقدرة أكثر مما يجب) وهي محل اهتمام الدراسة الحالية والباقي ٣٦ مشاهدة خاصة بالأتعاب غير العادية السالبة (أتعاب مقدرة أقل مما يجب). فضلاً عن عدم وجود أي مشاكل تتعلق بالازدواج الخطي وهي ما يتضح من نتائج الجدول رقم (١) التالي:

جدول رقم (١): نتائج تشغيل نموذج الأتعاب في البيئة المصرية

Model	β. Coef.	T	Sig.	VIF
(Constant)	8.338	8.258	.000	
lnTA	.138	3.295	.002	2.635
SQSUB	.042	.261	.795	2.353
FOREIGN	-.539	-1.682	.098	1.209
LnSEG	-.697	-2.217	.031	1.507
RECINV	-.223	-.741	.462	1.513
QUICK	-.101	-3.681	.001	2.195

LEV	.104	.289	.774	1.752
ROA	.985	2.451	.017	1.216
LOSS	.120	.457	.649	2.522
SGROWTH	-.019	-.270	.788	1.337
MTB	-.060	-.384	.702	3.198
SPEC	-.219	-.230	.819	1.332
INITIAL	-.138	-.734	.466	1.621
LnARLAG	.613	5.037	.000	1.395
YEND	.164	.405	.687	1.157
N	75			
Adj. R2	59.90%			
F-Value	8.36			
Durbin-Watson	1.072			

٣-٥-٢: الإحصاءات الوصفية:

يمكن للباحثان عرض الإحصاءات الوصفية لكافة المشاهدات بعينة الدراسة من خلال الجدول الخاص بالإحصاءات الوصفية على النحو التالي:

جدول رقم (٢): الإحصاءات الوصفية لمتغيرات الدراسة (ن = ٧٥)

	Min.	Max.	Mean	Std. Deviation	Skewness	Kurtosis
LnWords	1.281	5.481	3.618	1.412	0.685	1.311
LITIGIOUS	1.436	6.811	3.981	1.512	1.627	2.519
LnINS.CS	1.150	3.280	2.250	0.068	0.987	1.315
CI	0.000	1.000	0.027	0.015	1.457	1.634
Ln AF	1.220	0.990	1.115	0.670	0.030	1.322
PABAF	0.017	1.751	0.334	0.343	2.286	6.979
NABAF	-2.031	-0.025	-0.427	0.356	1.137	3.487
LNTA	13.925	23.889	20.570	2.913	-1.387	1.094
LEV	-0.060	0.806	0.426	0.197	-0.155	-0.066
ROA	-0.089	0.397	0.066	0.108	1.642	2.145
LOSS	0.000	1.000	0.489	0.111	-0.054	-1.143
BIG4	0.000	1.000	0.312	0.098	-0.052	-1.282

يتبين للباحثان من خلال العرض السابق للجدول رقم (٢) الخاص بالإحصاءات الوصفية مجموعة من الملاحظات التي يمكن توضيحها فيما يلي:

- يتبين اعتدال الوسط الحسابي للمتغيرات LnWords، LITIGIOUS الخاصة بتحليل المحتوى للإفصاح عن مخاطر الأمن السيبراني حيث يبلغ الوسط الحسابي

للقيمتين ٣,٦١٨، ٣,٩٨١ على التوالي، حيث أنهما يتوسطان القيمة بين الحدود الدنيا والقصوى.

- يبلغ الوسط الحسابي للمتغير CI الخاص بهجمات الأمن السيبراني ٢,٧% وهي نسبة نادرة جداً لوجود عدد ٢ مشاهدة فقط هم من اعترفوا بوجود هجمات الكترونية وعلى الموقع الالكتروني فقط ولم تفصح بذلك في التقارير والقوائم المالية.
- يتبين اعتدال الوسط الحسابي لقيمة الاستثمارات المدفوعة في التأمين ضد مخاطر الأمن السيبراني حيث يبلغ ٢,٢٥ بين قيمتي الحد الأدنى والأقصى ١,١٥، ٣,٢٨ على التوالي.
- فيما يتعلق بالمتغيرات الخاصة بأتعاب عملية المراجعة فيتبين انخفاض الأوساط الحسابية لمتغيرات الأتعاب الاجمالية وكذلك الأتعاب غير العادية الموجبة والسالبة حيث بلغت ١,١١٥، ٠,٣٣٤، -٠,٤٢٧ على التوالي.
- وأخيراً يتبين للباحثان انخفاض مستوى الانحراف المعياري للعينة وانحصار قيم معاملات الالتواء بين ± ٣ وانحصار قيم معاملات التفرطح بين ± ١٠ مما يشير إلي اعتدالية توزيع بيانات عينة الدراسة وعدم تشتتها.

٣-٥-٣: مصفوفة ارتباط بيرسون:

يحاول الباحثان في هذا الجزء من الدراسة الحالية تحليل أثر الإفصاح عن مخاطر الأمن السيبراني على أتعاب عملية المراجعة، وبخاصة في ظل تباين الطرق المختلفة لقياس الإفصاح عن مخاطر الأمن السيبراني، وبالتالي يهدف الباحثان في هذا الجزء من الدراسة إلي عرض مصفوفة ارتباط بيرسون بين المتغيرات المدرجة بنماذج اختبار الفروض الإحصائية من خلال الجدول رقم (٣) للتعرف على طبيعة العلاقة بين المتغيرات المستقلة وبعضها البعض بنماذج اختبار الفروض الإحصائية للدراسة، وتكوين رأي مبدئي عن مشكلة الازدواج الخطي بين تلك المتغيرات. بالإضافة إلي قيام الباحث بقياس معامل VIF للتأكيد على عدم تواجد أياً من مشاكل الازدواج الخطي.

جدول رقم (٣): مصفوفة ارتباط بيرسون (ن =٧٥)

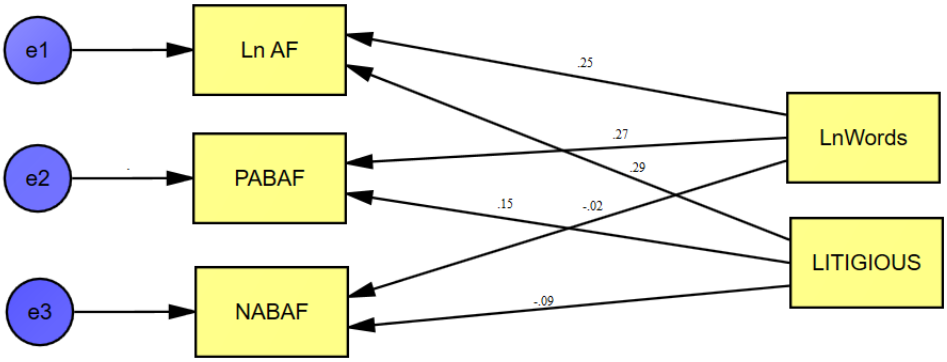
	LnWords	LITIGIOUS	INS.CS	CI	Ln AF	PABAF	NABAF	LNTA	LEV	ROA	LOSS	BIG4
LnWords	1											
LITIGIOUS	0.074	1										
INS.CS	0.071	0.110	1									
CI	0.097	0.273	0.132	1								
Ln AF	0.265	0.245	0.223	0.215	1							
PABAF	0.301	0.160	0.276	0.119	0.110	1						
NABAF	-0.086	-0.237	-0.171	-0.272	0.195	0.188	1					
LNTA	0.217	0.228	0.236	0.090	0.121	0.238	0.212	1				
LEV	0.275	0.261	0.195	0.118	0.127	0.056	0.283	0.158	1			
ROA	0.190	0.110	0.182	0.142	-0.109	-0.087	0.075	0.063	0.284	1		
LOSS	0.313	0.154	0.297	0.240	0.283	0.311	0.274	0.267	0.059	0.078	1	
BIG4	0.238	0.209	0.275	0.156	0.139	0.200	0.307	0.257	0.152	0.107	0.104	1

ويتضح لدى الباحثان من معاملات الارتباط المدرجة بالجدول (٣) عدم وجود أي علاقة بين المتغيرات المستقلة وبعضها البعض حيث لم يتبين وجود معاملات ارتباط أكبر من ٠,٨ ومن ثم لن تكون هناك أي مشكلة من مشاكل الازدواج الخطي بشرط حذف المتغيرين السابقين من النماذج سالفة الذكر.

٣-٥-٤: نتائج اختبارات الفروض الإحصائية:

- **نتيجة الفرض الإحصائي الأول:**

يهدف الباحثان في هذا الجزء من الدراسة إلي تحليل أثر الإفصاح عن مخاطر الأمن السيبراني على أتعاب عملية المراجعة بمكونيها من الأتعاب غير العادية الموجبة والسالبة بالتطبيق على عينة من الشركات المقيدة في سوق الأوراق المالية المصري. وذلك من خلال تشغيل نماذج اختبار الفروض الإحصائية للدراسة الحالية رقم (٢ ، ٣ ،٤)، ويمكن للباحثان التعبير عن نتائج اختبار ذلك الفرض باستخدام تحليل المسار ورسم النموذج من خلال الشكل رقم (١) التالي:



يتبين من الشكل السابق معنوية المسارات الخاصة باللوغاريتم الخاص بعدد كلمات الإفصاح عن مخاطر الأمن السيبراني وكذلك كلمات التقاضي فيما يتعلق بالتأثير على أتعاب عملية المراجعة، فضلاً عن معنوية اللوغاريتم الخاص بعدد كلمات الإفصاح عن مخاطر الأمن السيبراني على الأتعاب غير العادية الموجبة، وعدم معنوية بقية المسارات وتأكيداً على تلك النتائج يمكن للباحثان إجراء تحليل الانحدار المتعدد والتي تتضح نتائجه من خلال الجدول رقم (٤) التالي:

جدول رقم (٤): نتيجة اختبار الفرض الإحصائي الأول للدراسة

Variables	Panel (A) Dependent Variable: Ln AF			Panel (B) Dependent Variable: PABAF			Panel (C) Dependent Variable: NABAF		
	β Coef.	P-Value	T. Stat.	β Coef.	P-Value	T. Stat.	β Coef.	P-Value	T. Stat.
Cons.	0.028	0.077	1.401	0.050	0.062	1.816	0.133	0.114	1.442
LnWords	0.209	0.045	2.458	0.242	0.125	2.711	-0.020	0.117	-1.647
LITIGIOUS	0.259	0.032	2.111	0.141	0.027	1.458	-0.094	0.093	-1.612
LNTA	0.159	0.055	1.107	0.172	0.108	1.707	0.153	0.073	1.251
LEV	0.120	0.136	1.342	0.115	0.134	1.666	0.015	0.099	1.693
ROA	-0.153	0.150	-1.562	-0.071	0.106	-1.678	0.018	0.058	1.855
LOSS	0.136	0.108	1.494	0.024	0.130	1.075	0.030	0.075	1.166
BIG4	0.119	0.072	1.605	0.188	0.128	1.601	0.028	0.131	1.332
Fixed effects	*Included*			*Included*			*Included*		
N	75			39			36		
Adj. R2	36.20%			32.80%			29.60%		
VIF MAX	2.46			1.14			1.41		

يتبين للباحثان من خلال العرض الجدول رقم (٤) أن العمود الأول (Panel A) يشير إلي معنوية المتغيرين LnWords، LITIGIOUS الخاصين بتحليل المحتوى للإفصاح عن مخاطر الأمن السيبراني حيث أن (β = 0.209, 0.259, T =

(2 < 2.458, 2.111 وكلاهما يحمل إشارة موجبة مما يشير إلي وجود علاقة طردية بينهما وبين المتغير التابع الخاص بإجمالي أتعاب عملية المراجعة، أي أن زيادة مستوى الإفصاح عن مخاطر الأمن السيبراني تؤدي إلي زيادة مستوى أتعاب عملية المراجعة الإجمالية.

كما تشير نتائج العمود الثاني (Panel B) إلي معنوية المتغير LnWords الخاص بتحليل مستوى الإفصاح عن مخاطر الأمن السيبراني باستخدام عدد كلمات المخاطر حيث أن (β = 0.242, T = 2.711 > 2)، وعدم معنوية المتغير LITIGIOUS الخاص بتحليل المحتوى للافصاح عن مخاطر الأمن السيبراني باستخدام الكلمات القضائية حيث أن (β = 0.141, T = 1.458 < 2) وكلاهما يحمل اشارة موجبة مما يشير إلي وجود علاقة طردية بين الإفصاح عن مخاطر الأمن السيبراني باستخدام عدد كلمات المخاطر وبين المتغير التابع الخاص بإجمالي أتعاب عملية المراجعة، أي أن زيادة مستوى الإفصاح عن مخاطر الأمن السيبراني باستخدام عدد كلمات المخاطر تؤدي إلي زيادة مستوى أتعاب عملية المراجعة غير العادية الموجبة، بينما لا يوجد تأثير لتحليل المحتوى للإفصاح عن مخاطر الأمن السيبراني باستخدام الكلمات القضائية على مستوى أتعاب عملية المراجعة غير العادية الموجبة.

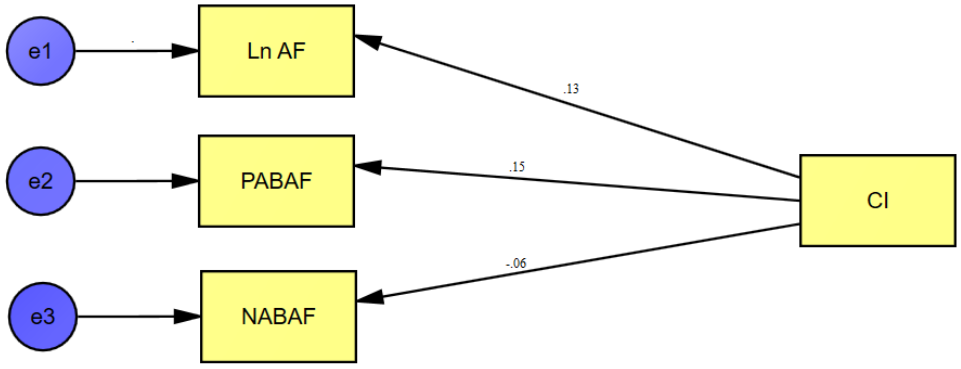
وأخيراً، تشير نتائج العمود الثالث (Panel C) إلي عدم معنوية المتغيرين LnWords، LITIGIOUS الخاصين بتحليل المحتوى للإفصاح عن مخاطر الأمن السيبراني حيث أن (β = -0.020, -0.094, T = -1.647, -1.612 < 2) مما يشير إلي عدم وجود علاقة بينهما وبين المتغير التابع الخاص بالأتعاب غير العادية السالبة لعملية المراجعة، أي أن زيادة مستوى الإفصاح عن مخاطر الأمن السيبراني لا تؤثر على مستوى الأتعاب غير العادية السالبة لعملية المراجعة.

وتأسيساً على ذلك، يتبين للباحثان قبول الفرض الإحصائي الأول للدراسة على الشكل البديل التالي:

يوجد تأثير ذو دلالة إحصائية للإفصاح عن مخاطر الأمن السيبراني باستخدام أسلوب تحليل المحتوى على أتعاب عملية المراجعة.

- **نتيجة الفرض الإحصائي الثاني:**

يهدف الباحثان في هذا الجزء من الدراسة إلي تحليل أثر تعرض الشركة للهجمات السيبرانية على أتعاب عملية المراجعة بمكونيها من الأتعاب غير العادية الموجبة والسالبة بالتطبيق على عينة من الشركات المقيدة في سوق الأوراق المالية المصري، وذلك من خلال تشغيل نماذج اختبار الفروض الإحصائية للدراسة الحالية رقم (٥ ، ٦ ، ٧). ويمكن للباحثان التعبير عن نتائج اختبار ذلك الفرض باستخدام تحليل المسار ورسم النموذج من خلال الشكل رقم (٢) التالي:



يتبين من الشكل السابق عدم معنوية المسارات الخاصة بتعرض الشركة للهجمات السيبرانية، ومن ثم عدم وجود أي تأثير لمثل هذه الهجمات على أتعاب عملية المراجعة بمكونيها (الأتعاب غير العادية السالبة والموجبة)، وتأكيداً على تلك النتائج يمكن للباحثان إجراء تحليل الانحدار المتعدد والتي تتضح نتائجه من خلال الجدول رقم (٥) التالي:

جدول رقم (٥): نتيجة اختبار الفرض الإحصائي الثاني للدراسة

Variables	**Panel (A)** Dependent Variable: Ln AF			**Panel (B)** Dependent Variable: PABAF			**Panel (C)** Dependent Variable: NABAF		
	β Coef.	P-Value	T. Stat.	β Coef.	P-Value	T. Stat.	β Coef.	P-Value	T. Stat.
Cons.	0.122	0.099	1.327	0.123	0.117	0.989	0.035	0.068	1.845
CI	0.125	0.090	1.356	0.145	0.068	1.631	-0.058	0.084	-1.370
LNTA	0.040	0.138	1.489	0.027	0.154	1.627	0.023	0.153	1.579
LEV	0.119	0.120	1.398	0.133	0.130	1.143	0.182	0.145	1.541
ROA	-0.094	0.134	-1.050	-0.100	0.105	-1.408	0.110	0.075	1.553
LOSS	0.187	0.120	1.539	0.074	0.069	1.675	0.127	0.061	1.330
BIG4	0.228	0.063	1.702	0.170	0.071	1.689	0.094	0.123	1.789
Fixed effects	*Included*			*Included*			*Included*		
N	75			39			36		
Adj. R2	33.60%			34.80%			31.40%		
VIF MAX	2.46			1.14			1.41		

يتبين للباحثان من خلال العرض للجدول رقم (٤) أن العمود الأول (Panel A) يشير إلي عدم معنوية المتغير CI الخاص بتعرض الشركة للهجمات السيبرانية حيث أن ($\beta = 0.125, T = 1.356 < 2$) مما يشير إلي عدم وجود علاقة معنوية بين تعرض الشركة للهجمات السيبرانية وأتعاب عملية المراجعة، أي أن زيادة مستوى تعرض الشركة للهجمات السيبرانية لا يؤثر على مستوى أتعاب عملية المراجعة.

كما تشير نتائج العمود الثاني (Panel B) إلي عدم معنوية المتغير CI الخاص بتعرض الشركة للهجمات السيبرانية حيث أن ($\beta = 0.145, T = 1.631 <$ 2) مما يشير إلي عدم وجود علاقة معنوية بين تعرض الشركة للهجمات السيبرانية وأتعاب عملية المراجعة غير العادية الموجبة. أي أن زيادة مستوى تعرض الشركة للهجمات السيبرانية لا يؤثر على مستوى أتعاب عملية المراجعة غير العادية الموجبة.

وأخيراً، تشير نتائج العمود الثالث (Panel C) إلي عدم معنوية المتغير CI الخاص بتعرض الشركة للهجمات السيبرانية حيث أن ($\beta = -0.058, T = -1.370$ 2 <) مما يشير إلي عدم وجود علاقة معنوية بين تعرض الشركة للهجمات السيبرانية وأتعاب عملية المراجعة غير العادية السالبة، أي أن زيادة مستوى تعرض الشركة للهجمات السيبرانية لا يؤثر على مستوى أتعاب عملية المراجعة غير العادية السالبة.

وتأسيساً على ذلك، يتبين للباحثان قبول الفرض الإحصائي الثاني للدراسة على الشكل البديل التالي: ***لا يوجد تأثير ذو دلالة إحصائية لتعرض الشركة للهجمات السيبرانية على أتعاب عملية المراجعة.***

وبناء على ما سبق يمكن توضيح أن المخاطر والقيم المعرضة للخطر فيما يتعلق بالهجمات السيبرانية تشتمل على العديد من الخسائر المحتملة والتي تتمثل في التكاليف المتكبدة نتيجة تلك الهجمات، ومن ثم يصبح علي الشركة استخدام الشفافية مع الأطراف الخارجية ذوي المصلحة بالشركة والإفصاح عن تلك الخسائر والتكاليف المتكبدة نتيجة هذه الهجمات السيبرانية، وفي هذا الشأن تتطور مسئولية المراجع إلي مراجعة تلك الإفصاحات وابداء الرأي الفني المحايد بشأنها، ومن ثم يستلزم الأمر تطوير الممارسات المهنية للمراجع في هذا الشأن وهو ما يؤدي إلي زيادة مستوى الأتعاب المطلوبة لمراجعة تلك الأنظمة التكنولوجية الجديدة. وبناء على ذلك يؤكد الباحثان اعتماده على تحليل محتوى نماذج الإفصاح عن مخاطر الأمن السيبراني في البيئة المصرية باعتباره أحد العوامل الهامة التي تفسر العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب عملية المراجعة، حيث تشير هذه النماذج إلى مدى

وجود مخاطر للهجمات السيبرانية من عدمه الأمر الذى يؤدى بدورة إلى زيادة جهد عملية المراجعة وبما ينعكس على أتعاب المراجع الخارجي .

القسم الرابع : النتائج والتوصيات والدراسات المستقبلية

٤-١ النتائج:

- يترتب على حوادث الأمن السيبراني تكاليف غير المباشرة قد تتمثل في فقدان فرص العمل، خفض الإيرادات، وفقد ثقة العملاء يصعب تحديد كميتها بشكل موضوعي وتشمل درجة أكبر من مخاطر عملية المراجعة، وتحتاج من المراجع المزيد من الجهد المبذول ويقابل هذا الجهد أتعاب مراجعة مرتفعة .
- إن حوادث الأمن السيبراني اللاحقة التي تحدث بعد إصدار تقرير فحص الأمن السيبراني يمكن أن توفر إشارة خارجية سلبية للمستثمرين حول جودة التأكيد الخارجي.
- يوفر وجود إطار عمل للإفصاح عن مخاطر الأمن السيبراني لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للشركة وفعالية برنامج إدارة المخاطر الخاص بها.
- اتفقت النتائج النظرية مع نتائج الدراسات السابقة في أن المراجعين عوضوا بشكل فعال الزيادات في مخاطر المراجعة من خلال الاختبارات الجوهرية وجهد المراجعة بما يدعم وجهه النظر بأن مراجعي الحسابات زادوا من وعيهم بمخاطر المراجعة ووضعوا إجراءات مناسبة للتعامل مع عواقب حوادث الأمن السيبراني.
- توصلت النتائج النظرية إلى أن الخسارة المتوقعة من الارتباط بعميل محفوف بالمخاطر تزيد من مخاطر أعمال المراجع مثل ضعف السمعة وعدم تحصيل الأتعاب، ولذا فإن شركات المراجعة تأخذ في الاعتبار مخاطر الأعمال في عمليات تسعير المراجعة وأن الشركات تفرض أتعاب مراجعة إضافية عندما تكون مخاطر العمل عالية .

- كما توصلت النتائج النظرية إلى أنه من الممكن تعزيز جاذبية استثمارات الشركة من خلال إصدار تقرير تأكيد مستقل بمفرده، وأن الأمن السيبراني يمثل مصدر قلق كبير للإدارة وأعضاء مجلس الإدارة والمستثمرين غير المحترفين والمنظمين.
- يوجد ارتباط إيجابي بين أتعاب عملية المراجعة ومخاطر اختراقات الأمن السيبراني، وتتفق هذه النتيجة مع العديد من الدراسات في أن مراجعي الحسابات عندما يجدون المزيد من مخاطر الأمن السيبراني يبذلون المزيد من الجهد أثناء عملية المراجعة الأمر الذى يؤدى إلى فرض أتعاب مرتفعة.
- تقيم شركات المراجعة مخاطر هجمات الأمن السيبراني ليس فقط من خلال تقييم حوادث الاختراق السيبراني الفعلية ولكن أيضاً من خلال عمليات الإفصاح عن مخاطر الأمن السيبراني بشكل عام، مما يؤثر على أتعاب مراجع الحسابات وهو ما يدعم الفرض الأول والذى ينص على وجود تأثير ذو دلالة إحصائية للإفصاح عن مخاطر الأمن السيبراني باستخدام أسلوب تحليل المحتوى على أتعاب عملية المراجعة.
- لا توجد علاقة معنوية بين تعرض الشركة للهجمات السيبرانية وأتعاب عملية المراجعة، أي أن زيادة مستوى تعرض الشركة للهجمات السيبرانية لا يؤثر على مستوى أتعاب عملية المراجعة.

٤-٢ التوصيات والدراسات المستقبلية:

- يجب أن تأخذ المنظمات في الاعتبار ديناميكيات الأعمال المتغيرة بسرعة ليس فقط للتكيف بفعالية ولكن أيضاً لتطبيق منهج متكامل لعملية ضمان الأمن السيبراني بكفاءة بناءً على أفضل الممارسات.

- زيادة الوعى بمخاطر هجمات الأمن السيبراني من خلال توفير إطار عمل للإفصاح عن مخاطر الأمن السيبراني، بما يمكن أصحاب المصلحة من تقييم موقف الأمن السيبراني للشركة.
- تنسيق ومواءمة تأكيدات الأمن السيبراني مع السياسات التنظيمية لدعم وتسهيل التعاون الاستراتيجي وتبادل المعلومات بين وحدات الأعمال والموظفين ذوي الصلة في بيئة العمل اليومية.
- استحداث إطار عمل لمراقبة الأمن السيبراني ففي بيئة الأعمال الحالية عادة ما يكون لدى المؤسسات إطار عمل قديم أو غير مكتمل للاستجابة للمخاطر، لذا لابد من استحداث إطار جديد يركز بشكل كبير على تكنولوجيا المعلومات.
- الاعتماد على منهج تحليلات البيانات حيث يعد هو المنهج الحاسم لضمان الأمن السيبراني والهدف الرئيسي هو أن تكون المنظمات قادرة على نقل المعلومات بسرعة ، من خلال الحفاظ على الجودة العالية والأمن.
- إجراء المزيد من الدراسات المستقبلية عن العلاقة بين استخدام منهج تحليلات البيانات الضخمة على الحد من مخاطر هجمات الأمن السيبراني: أدلة من شركات الأقمار الصناعية.
- إجراء المزيد من الدراسات المستقبلية حول تفسير العلاقة بين الأبعاد المتعددة لمخاطر الأمن السيبراني على الاختيار التكيفي لاستراتيجيات ضبط وقياس التحريفات الجوهرية في القوائم المالية لشركات تكنولوجيا المعلومات.
- إجراء المزيد من الدراسات المستقبلية عن دور آليات الحوكمة الداخلية في التنبؤ بالمعلومات المستقبلية لمخاطر الأمن السيبراني.

قائمة المراجع

المراجع باللغة العربية:

١- فرج، هاني خليل، " أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الامن الإلكتروني على قرارات الاستثمار بالأسهم – دراسة تجريبية"، ***مجلة المحاسبة والمراجعة*** ، مجلة دولية تصدر عن كلية التجارة جامعة بنى سويف بالشراكة مع اتحاد الجامعات العربية، العدد ١١ ،٢٠٢٢، ١٢٩-٢٠٩.

المراجع باللغة الإنجليزية:

1. Ahmad, F., Bradbury, M., & Habib, A. (2021). Political connections, political uncertainty and audit fees: evidence from Pakistan. ***Managerial Auditing Journal***.73(2),255-282.
2. American Institute of Certified Public Accountants (AICPA) (2018). Cyber security risk management reporting fact sheet. (Accessed 12 November 2020). Available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-factsheet.pdf .
3. Asthana, S., Kalelkar, R., Raman, K., (2021). Does client cyber-breach have reputational consequences for the local audit office? ***Account. Horizon***. 35 (4): 1–22.
4. Bao Ngo, T. N., & Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. Interdisciplinary Description of Complex Systems: INDECS, 19(3), 375-390.
5. Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. ***Journal of Accounting and Public Policy***, 106998.

6. Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes. MIS Quarterly, Forthcoming.
7. Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. ***Journal of Accounting and Public Policy***,37(6), 508–526.
8. Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). Equifax says cyberattack may have affected 143 million in the US. The New York Times, A1. Bourdon, B. (2019), "The adorable mistakes executives continue to make after a data breach," ***Harvard Business Review***, Press, Boston.
9. Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. ***International Journal of Auditing***, *25*(1), 24-39.
10. Center for Audit Quality: *Cybersecurity and the External Audit.*CAQ Alert ,2014-3, Center for Audit Quality, Washington D.C., 2014, http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit, accessed 19th December 2019,
11. Chi, W., Lisic, L. L., Myers, L. A., Pevzner, M., & Seidel, T. A. (2022). Does Visibility of an Engagement Partner's Association with Recent Client Restatements Increase Fee Pressures from Non-Restating Clients?. ***Accounting Horizons***, 36(2), 19-45.
12. Chu, J., Qin, X., & Fang, J. (2018). Economic policy uncertainty and auditors' decisions: evidence based on audit fees. ***Accounting Research***, 374(12), 85-91.
13. Corbet, S. and C. Gurdgiev. 2019. What the hack: Systematic risk contagion from cyber events. ***International Review of Financial Analysis***, 65: 1-18.

14. Dennis, A., Wixom, B.H., & Tegarden, D. (2015). Systems analysis and design: An objectoriented approach with UML. John Wiley & Sons.
15. Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. ***Journal of Information Systems***, *33*(3), 183-200.
16. Griffiths, J. (2015). "Cybercrime costs the average U.S. firm $15 million a year." *CNN Money* .
17. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. ***Managerial Auditing Journal***, 34(7), 808-834.
18. Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing Organizational Legitimacy Following Information Technology (IT) Material Weaknesses: Executive Turnover, IT Expertise, and IT System Upgrades. ***Journal of Information Systems***, 30(1),41-70.
19. Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. In Workshop on the Economics of Information Security (WEIS) .1:37
20. Hamm, K. (2019). Cybersecurity: Where We Are; What More Can be Done? A call for auditors to lean in. Available at: https://pcaobus.org/ News/Speech/Pages/hamm-cybersecurity-where-we-are-what-morecan be done.aspx.
21. Hansen, J. C., Murray, S. M., Park, S. H., & Shin, N. (2022). Judicial hellholes and other differential characteristics: is state-level legal risk reflected in audit fee pricing?. ***Managerial Auditing Journal***
22. Heller, M. 2017. "Cyber attacks can cause major stock drops." *CFO.com* April 12, 2017.

23. Héroux, S., and Fortin, A. (2020), "Cybersecurity disclosure by the companies on the S&P/TSX 60 Index", ***Accounting Perspectives***, 19 (2): 73-100.
24. Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between boardlevel technology committees and reported security breaches. ***Journal of Information System****s*.30(3): 79-98.
25. Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. ***Information & Management*** 52 (3): 337–347.
26. Hossain, S., & Wang, J. J. (2022). Abnormal audit fees and audit quality: Australian evidence. ***Australian Journal of Management***, 03128962221093831
27. Hsieh, T. S., Kim, J. B., Wang, R. R., & Wang, Z. (2020). Seeing is believing? Executives' facial trustworthiness, auditor tenure, and audit fees. ***Journal of Accounting and Economics***, 69(1), 101260.
28. Hsu, C., Wang, T., Lu, A., 2016. The Impact of ISO 27001 Certification on Firm Performance. In: Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii .
29. Joe, J. R., Janvrin, D. J., Barr-Pulliam, D., Mason, S., Pitman, M. K., Rezaee, Z., Sanderson, K.-A., & Wu, Y.-J. (2015). The Auditing Standards Committee of the Auditing Section of the American Accounting Association is Pleased to Provide Comments on PCAOB Staff Consultation Paper No. 2015-01, The Auditor's Use of the Work of Specialist s: Participating Committee Members. Current Issues in Auditing, 9(2), C18-C37.
30. Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. ***Managerial Auditing Journal***.

31. Kajüter, P., Klassmann, F., & Nienhaus, M. (2016). Do Reviews by External Auditors Improve the Information Content of Interim Financial Statements?. ***The International Journal of Accounting***, 51(1), 23-50.
32. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the Impact of Successful Cyberattacks on Target Firms? (No. w24409). National Bureau of Economic Research.
33. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation,and the impact of successful cyberattacks on target firms. ***Journal of Financial Economics***.
34. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). National Bureau of Economic Research.
35. Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. ***Journal of Information Systems***, *34*(3), 133-157.
36. Khalil, S., and M. Mazboudi. (2016). Client acceptance and engagement pricing following auditor resignations in family firms. ***Auditing: A Journal of Practice & Theory*** ,35 (4): 137–158.
37. Krus, C. M. (2012), "Who is listening? The SEC emphasizes importance of cybersecurity disclosure", ***Journal of Investment Compliance***, 13 (1) , 30-32.
38. Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is Operational Control Risk Informative of Financial Reporting Deficiencies?. ***Auditing: A Journal of Practice & Theory***, 37(1), 139-165.
39. Li, H., Huang, F., Sun, Z., & Wang, T. D.(2020). Auditors' Cybersecurity Breach Experience on Non-Breached Clients' Audit Fees. Available at SSRN 4082411.

40. Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? ***Evidence from audit fees. Auditing****: A Journal of Practice & Theory*, *39*(1), 151-171.
41. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cyber security risk factors. ***International Journal of Accounting Information Systems,*** *30*, 40-55.
42. Lim, Y., & Monroe, G. S. (2022). Analyst Coverage and Audit Fees: International Evidence. ***Journal of Accounting, Auditing & Finance***, *37*(2), 466-492.
43. Masoud, N., & Al-Utaibi, G. (2022). The Determinants of Cybersecurity Risk Disclosure in Firms' Financial Reporting: Empirical Evidence. ***Research in Economics***.
44. McKenna, F., (2019). Equifax auditors are on the hook for data security risk controls. *Retrieved from marketwatch. Com*.
45. Mitra, S., Jaggi, B., & Al-Hayale, T. (2019). Managerial overconfidence, ability, firm-governance and audit fees. ***Review of Quantitative Finance and Accounting***, *52*(3), 841–870.
46. Mohan, V., Simon, D., Rosenfeld, R., and Brown, M. (2021), "SEC increasingly turns focus toward strength of cyber risk disclosures", available at: https://corpgov.law.harvard.edu/2021/07/25/sec-increasingly-turns-focus-towardstrength-of-cyber-risk-disclosures/ (accessed 25 November 2021).
47. Morgan, S. (2018). Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018. Available at: http://bit.ly/30Oc3VE
48. Muniandy, B. (2022). Audit fees, board ethnicity and board independence: evidence from South Africa. *Managerial Auditing Journal*.

49. Pacheco-Paredes, A., & Wheatley, C. M.(2022), Do Auditors Consider Cybersecurity Insurance in Pricing Audits?. Available at SSRN 4171153.
50. Pendley, J. A. (2018), "Finance and accounting professionals and cybersecurity awareness",***The Journal of Corporate Accounting and Finance,*** 29 (1): 53-58.
51. Perols, R. R., & Murthy, U. S. (2021). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. ***Auditing: A Journal of Practice & Theory***, *40*(1), 73-89.
52. Prabhawa, A. A., & Nasih, M. (2021). Intangible assets, risk management committee, and audit fee. ***Cogent Economics & Finance***, 9(1), 1956140.
53. PricewaterhouseCoopers (PWC). 2016. Turnaround and transformation in cyber security: Retail and consumer key findings from The Global State of Information Security Survey 2016. Available at: https://www.pwc.ru/en/retail- onsumer/publications/assets/2016_ gsiss_rc.pdf
54. Richardson, V., Watson, M. W., Smith, R. E., (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *J. Inf. Syst*. 33 (3): 227–265.
55. Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019a). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. ***Research in International Business and Finance***,*47*, 458–469.
56. Rosati, P., Deeney, P., Gogolin, F., Cummins, M., Van der Werff, L., & Lynn, T. (2017). The Effect of Data Breach Announcements Beyond The Stock Price: Empirical Evidence on Market Activity. ***International Review of Financial Analysis***, 49, 146-154.

57. Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. ***The International Journal of Accountin****g*, 54(03), 1950013
58. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. ***European Accounting Review***, 31(3), 701-728.
59. Securities and Exchange Commission: *Commission Statement and Guidance on Public Company Cybersecurity Disclosures.* Securities and Exchange Commission, 17 CFR Parts 229 and 249, Washington D.C., 2018, https://www.sec.gov/rules/interp/2018/33-10459.pdf, accessed 13th December 2019,
60. Securities and Exchanges Commission – SEC (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. (February 2018) Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accessed December 19, 2018).
61. Smith, D. D., Gleason, K. C., & Kannan, Y. H. (2021). Auditor liability and excess cash holdings: Evidence from audit fees of foreign incorporated firms. ***International Review of Financial Analysis***, *78*, 101947.
62. Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do Auditors Price Breach Risk in Their Audit Fees? ***Journal of Information Systems***, 33(2).
63. Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, 58, 216-229.
64. Tosun, O. K. (2021). Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, 101795.

65. Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. ***International Journal of Accounting & Information Management***.

66. Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. ***Journal of Accounting and Public Policy***, 37(6), 489-507.