تأثير جرائم الأمن السيبراني على مخاطر المراجعة وإنعكاسه على أتعاب المراجعة (دراسة تطبيقية)

دنيا محمد قاسم سالم

تحت إشراف

الأستاذ الدكتور/ أشرف محمد إبراهيم منصور

أستاذ المراجعة بكلية التجارة وإدارة الأعمال – جامعة حلوان

ملخص البحث

يهدف البحث إلى تحديد تأثير جرائم الأمن السيبراني على أتعاب المراجعة، وذلك في ظل وجود مخاطر المراجعة كمتغير وسيط. ولتحقيق هذا الهدف تم إجراء دراسة تطبيقية على شركات قطاع الإتصالات والإعلام وتكنولوجيا المعلومات المقيدة في البورصة المصرية، وذلك خلال الفترة الزمنية ٢٠١٧-٢٠٢٠. وأظهرت نتائج الدراسة أنه يوجد تأثير معنوي وطردي لجرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية ومخاطر المراجعة. بالإضافة إلى ذلك، توصلت الدراسة إلى أن مخاطر المراجعة "تتوسط" العلاقة بين جرائم الأمن السيبراني وأتعاب المراجعة.

الكلمات المفتاحية: جرائم الأمن السيبراني، مخاطر المراجعة، أتعاب المراجعة.

The Effect of Cyber-Security Incidents on Audit Risks and its Reflection on Audit Fees

(An Applied Study)

Abstract

This research aims to identify the effect of cyber-security incidents on the audit fees in the presence of audit risks as a mediator variable. To achieve this goal, an applied study was conducted on information technology, media & communication

services companies listed on the Egyptian Stock Exchange, during the period from ٢٠١٧ to ٢٠٢٠. The results showed that the cyber-security incidents had a significant positive effect on audit fees and audit risks. As well as, the study concluded that audit risks "mediates" the relationship between cyber-security incidents and audit fees.

Keywords: Cyber-Security incidents, audit risks, audit fees.

١ـ مقدمة

أدى وقوع العديد من المتغيرات والتي منها ظاهرة العولمة والحوكمة وتعرض العالم لجائحة كورونا، إلى اعتماد معظم المنشأت في جميع أنحاء العالم بشكل أكبر على التكنولوجيا، مما فتح المجال لحفظ ونقل المعلومات إلكترونياً. لذلك، انتقل مفهوم حماية المعلومات من الحماية المادية والتي تتم من خلال توفير الوسائل المادية مثل الأقفال وغيرها من وسائل الحماية المادية، إلى الحماية الإلكترونية، مما دعا معظم منشأت الأعمال إلى ضرورة إيجاد سياسات وأساليب للحفاظ على جميع مواردها، وخاصةً الموارد المعلوماتية.

وفي هذا السياق، ظهرت العديد من السياسات المتعلقة بأمن المعلومات والحفاظ على سريتها، فأوجدوا ما يسمى بالأمن السيبراني**"Cyber Security"**. ويشمل مفهوم الأمن السيبراني: أمن المعلومات، الأمن الإلكتروني، الأمن الرقمي ونحو ذلك. (هيئة الاتصالات وتقنية المعلومات السعودي، ٢٠٢٠). ويعتبر الأمن السيبراني إحدى آليات حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.

ومع تزايد عدد جرائم الأمن السيبراني كل عام؛ نتيجة الاستخدام المتزايد للإنترنت، وتطبيقات الهاتف المحمول والتقنيات الحديثة، أصبح الأمن السيبراني يمثل أحد أهم القضايا للمنشأت في جميع الصناعات والبلدان (Corradini, ٢٠٢٠). حيث

يمكن لجرائم الأمن السيبراني أن تؤدي إلى ضرر كبير للشركات المُخْتَرِقَة من حيث الغرامات والسمعة (Cavausoglu et al., ٢٠٠٤; Gordon et al., ٢٠١١; Rosati et al., ٢٠١٩). لذا، يعتبر الأمن السيبراني من الوسائل الحديثة التي تستخدم في حماية المعلومات المربوطة بشبكة الإنترنت وتكنولوجيا المعلومات، حيث يحافظ على المعلومات من أي سرقة أو دخول غير مصرح على الأنظمة التي تخص منظمات الأعمال (السرحان، (٢٠٢٠.

وتؤكد "Ginni Rommetty" (المدير والرئيس التنفيذي الحالي لشركة أي بي إم) على أن جرائم الأمن السيبراني، تمثل التهديد الأعظم حالياً لأي منشأة في العالم لذلك، يتعين على جميع المنشأت الاستعداد وتجهيز بيئاتها الداخلية لذلك، ومحاولة منع الهجمات الإلكترونية التي قد تؤدي إلى إختراق بياناتها، خاصةً السرية منها. وعادةً ما تكون جرائم الأمن السيبراني إشارة على ضعف هيكل الرقابة الداخلية المطبق والموجود في المؤسسة (Chernobai et al., ٢٠١١; Benaroch et al., ٢٠١٢; Benaroch & Chernobai, ٢٠١٧). لذلك من الممكن أن تؤثر جرائم الأمن السيبراني بشكل جوهري على مخاطر أعمال المنشأة محل المراجعة ومخاطر المراجعة، الأمر الذي قد ينعكس في النهاية على أتعاب عملية المراجعة. ويرجع ذلك إلى أن تعرض منشأة عميل المراجعة لجرائم الأمن السيبراني يتطلب مزيد من الدقة عند التخطيط لعملية المراجعة نتيجة لإحتمالية زيادة مخاطر أعمال المنشأة ومخاطر المراجعة وبالتالي، بذل المزيد من الجهد وكذلك الاختبارات للتأكد من أن هيكل الرقابة الداخلية على التقارير المالية لم يتم المساس به (Calderon & Gao, ٢٠٢٠). ومع إجراء المزيد من الاختبارات سوف يؤدي ذلك إلى زيادة العمل الذي يقوم به المراجع. وبما أن أتعاب عملية المراجعة هي إنعكاس للجهد المبذول من قبل المراجع فمن المرجح أن يؤدي ذلك إلى زيادة أتعاب عملية المراجعة.

وفي نفس السياق أوضحتKathleen Hamm، وهي خبيرة في التكنولوجيا المالية والأمن السيبراني وعضو سابق في (PCAOP) أنه إذا قام المراجع بتحديد مخاطر مرتبطة بالأمن السيبراني للعميل والتي من الممكن أن يكون لها تأثير جوهري على القوائم المالية الخاصة بالشركة، يجب عليه تصميم وتنفيذ الإجراءات لتحديد تلك

المخاطر، ثم أوضحت بعد ذلك أنه سواء قد وقع حادث أم لا أثناء التخطيط لعملية المراجعة، يجب على المراجع إجراء تقييم للمخاطر ويجب أن يأخذ هذا التقييم في عين الاعتبار أي مخاطر للأمن السيبراني، والتي من الممكن أن يكون لها تأثير جوهري على القوائم المالية الخاصة بالمنشأة، لذلك من المتوقع زيادة عدد ساعات عمل المراجعة عند تعرض المنشأة للجرائم السيبرانية، مما سوف يؤدي إلى زيادة أتعاب عملية المراجعة (Hamm, ٢٠١٩).

٢ـ مشكلة البحث

ناقشت دراسة Bianchi et al., (٢٠١٩) أثر الإفصاح عن التهديدات والهجمات السيبرانية على الشركات وسوق رأس المال وذلك في الأجل القصير والأجل الطويل. وتوصلت الدراسة إلى أنه عندما تقوم الشركة بالإفصاح عن هجوم سيبراني لأول مرة فإنه توجد آثار على المدى القصير وآثار على المدى الطويل، بالنسبة للأثار على المدى القصير فإنها تتمثل في انخفاض العوائد اليومية غير العادية وزيادة حجم التداول بسبب ضعف البيع وتتدهور السيولة. وعلى المدى الطويل - حتى خمس سنوات تقريباً - تتأثر سياسات الشركة نتيجة الأضرار الكبيرة على سمعة الشركات، ومع الأخذ في الاعتبار فرضية كفاءة السوق والتي طورها Eugene Fama ومفادها أن أسعار الأسهم في سوق الأوراق المالية الكفء تعكس جميع المعلومات المتوفرة والمتعلقة بالسوق، وبالتالي فهي محصلة أراء جميع المستثمرين. لذلك ربما ستلجأ الشركة إلى إخفاء أي معلومات متعلقة بتعرضها للجرائم السيبرانية. وهنا يأتي السؤال فيما يتعلق بالدور الذي يقوم به المراجع الخارجي في حالة مراجعة الشركات التي تعرضت بالفعل للجرائم السيبرانية، هل سوف يضع هذا مزيد من الضغط على المراجع بسبب إحتمالية زيادة مخاطر أعمال المنشأة، ومخاطر المراجعة، ومع بذل المزيد من الجهد من قبل المراجع لتخفيض خطر المراجعة إلى مستوى مقبول، هل سوف يؤدي ذلك إلى فرض أتعاب مراجعة أعلى وذلك لجهودهم الرقابية العالية؟

وتوجد ندرة نسبية في الدراسات المتعلقة بجرائم الأمن السيبراني في مجال المراجعة وخاصةً في البيئة المصرية، وذلك على الرغم من أهمية هذا المجال وتأثيره الواضح؛ حيث تعد جرائم الأمن السيبراني من أكثر خمسة تهديدات تواجه الإقتصاد

العالمي (WEF, ٢٠١٧)، ومن أكثر عشرة تهديدات تواجه الشركات ومستقبلها وتفقد الأطراف المختلفة (المستثمرون,العملاء,الموردون وغيرهم) الثقة ليس فقط في الشركة التي تعرضت لحوادث وإختراقات أمن سيبرانية ولكن في الصناعة التي تنتمي إليها المنشأة بأكملها. لذا، تتمثل المشكلة الرئيسية للدراسة في وجود ندرة نسبية في الدراسات التي تناولت أثر جرائم الأمن السيبراني على أتعاب المراجعة، وذلك في وجود متغير وسيط هو مخاطر المراجعة. ويمكن إعادة صياغة مشكلة الدراسة في **التساؤل الرئيسي** التالي:

ما هو تأثير جرائم الأمن السيبراني على أتعاب المراجعة، وذلك في ضوء متغير وسيط هو مخاطر المراجعة؟

ويتفرع من هذا التساؤل الرئيسي، **التساؤلات** الآتية:

- ما هو تأثير جرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية؟
- ما هو تأثير جرائم الأمن السيبراني على مخاطر المراجعة؟
- ما هو تأثير مخاطر المراجعة على أتعاب مراجعة القوائم المالية؟
- إلى أى مدى تؤثر جرائم الأمن السيبراني بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة؟

٣- أهداف البحث

يعتبر الهدف الرئيسي للبحث هو تحديد تأثير جرائم الأمن السيبراني على أتعاب المراجعة، وذلك من خلال اعتبار مخاطر المراجعة كمتغير وسيط. ويتفرع من هذا الهدف الآتي:

١- تحديد تأثير جرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية.
٢- تحديد تأثير جرائم الأمن السيبراني على مخاطر المراجعة.
٣- تحديد تأثير مخاطر المراجعة على أتعاب مراجعة القوائم المالية.
٤- تحديد إلى أي مدى تؤثر جرائم الأمن السيبراني بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة.

٤ـ أهمية البحث

تتمثل **الأهمية العلمية** للبحث في تناوله لمجال هام، يعانى من ندرة بحثية في الممارسة المهنية وبيئة الأعمال المصرية، وهو الأمن السيبراني بشكل عام والجرائم المتعلقة به بشكل خاص وتلك الندرة البحثية ليست فقط في مصر حيث أن الموضوع لم يتم تناوله بشكل كافي حتى الآن (Haapamäki, ٢٠١٩). لذا، يستمد هذا البحث أهميته من أهمية القضية البحثية التي يتناولها والتي تتعلق بتحديد تأثير جرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية. وذلك من خلال اعتبار مخاطر المراجعة كمتغير وسيط. ويستمد البحث **أهميته العملية** من الفائدة التي ستعود على الأطراف الأساسية للمراجعة، خاصةً طرفي التعاقد على المراجعة، وتحديداً كل من المراجعين (بإعتبارهم مقدمي خدمة المراجعة)، وعملاء المراجعة (بإعتبارهم طالبي خدمة المراجعة)، عند تحديد أتعاب المراجعة؛ ويفيد المنظمات المهنية المسئولة عن تنظيم مزاولة المهنة في ضرورة الإستعداد لجرائم الأمن السيبراني.

٥ـ حدود البحث

يركز البحث على أتعاب مراجعة القوائم المالية السنوية الكاملة، ولن يتم تناول تأثير جرائم الأمن السيبراني على أتعاب الخدمات الأخرى التي تقدمها مكاتب المراجعة غير خدمة مراجعة القوائم المالية. وتقتصر الدراسة التطبيقية على عينة من شركات قطاع الإتصالات والإعلام وتكنولوجيا المعلومات المقيدة في البورصة المصرية، وذلك خلال الفترة الزمنية ٢٠١٧- ٢٠٢٠. ويحكم اختيار الشركات التي تتضمنها عينة الدراسة خلال الفترة من ٢٠١٧ حتى ٢٠٢٠ المحددات التالية: توافر محاضر اجتماعات الجمعيات العامة للشركات محل الدراسة وتقارير مجالس الإدارة وذلك خلال سنوات الدراسة من أجل الحصول على قيمة الأتعاب السنوية للمراجع؛ توافر القوائم المالية والإيضاحات المتممة لها خلال سنوات الدراسة؛ وأن تقوم الشركات محل الدراسة بنشر قوائمها المالية بالعملة المحلية المصرية (الجنيه المصري)؛ والأ تكون الشركة قد تعرضت للشطب أو التوقف؛ وأن يكون مضى على قيدها سنة أو أكثر وذلك خلال فترة الدراسة.

٦- منهجية البحث:

لتحقيق هدف البحث، سوف يتم الإعتماد على **أسلوب تحليل المحتوى** (Content Analysis) بالدراسة التطبيقية إلى جانب المقابلات الشخصية لتحديد أي إستفسار. وسوف يتم تحليل القوائم المالية السنوية، الإيضاحات المتممة للقوائم المالية، محاضر اجتماعات الجمعيات العامة ومجالس الإدارة، وذلك لمنشأت قطاع الإتصالات والإعلام وتكنولوجيا المعلومات المقيدة في البورصة المصرية، خلال الفترة الزمنية ٢٠١٧-٢٠٢٠.

٧- خطة البحث

في ضوء مشكلة البحث والهدف منه وفي إطار حدوده، سوف يُستكمل البحث كالتالي:

٧-١ ماهية وطبيعة جرائم الأمن السيبراني (المفهوم والخصائص).

٧-٢ مفهوم ومكونات مخاطر المراجعة.

٧-٣ العلاقة بين مخاطر المراجعة وجرائم الأمن السيبراني.

٧-٤ أتعاب المراجعة في ظل جرائم الأمن السيبراني.

٧-٥ الدراسات السابقة واشتقاق فرضيات البحث.

٧-٦ الدراسة التطبيقية.

٧-١ ماهية وطبيعة جرائم الأمن السيبراني:

يعتبر مصطلح جرائم الأمن السيبراني من المصطلحات الحديثة، وكان يوجد جدل كبير حول أفضل الطرق لتعريف جرائم الأمن السيبراني وذلك عندما بدأت في الظهور كتهديد، وفي البداية كان يوجد ميلًا إلى اعتبار أي جريمة تتعلق بجهاز كمبيوتر جريمة سيبرانية (Drew, ٢٠٢٠). وعلى الرغم من الانتشار الواسع للجرائم السيبرانية في الوقت الحالي نتيجة زيادة إستخدام الإنترنت وأدوات الإتصال الحديثة، لم يتم تطوير تعريف رسمي متسق عالمياً لجرائم الأمن السيبراني حتى الآن، حيث يوجد في الوقت الحالي العديد من التعريفات العامة ولكن لا يوجد تعريف تم

الإتفاق عليه عالمياً. وفيما يلي سوف نتطرق إلى بعض المفاهيم المختلفة، التي تم تقديمها من قبل بعض الباحثين.

وفقاً لدراسة Donalds & Bryson (٢٠١٩) تتضمن جرائم الأمن السيبراني عددًا كبيرًا من الأفعال، الجرائم، أو السلوك غير المشروع الذي يتم إرتكابه من قبل الأفراد أو الجماعات ضد أجهزة الكمبيوتر، الأجهزة المرتبطة بالكمبيوتر، أو شبكات تكنولوجيا المعلومات، وكذلك الجرائم التقليدية التي يتم تسهيلها أو الحفاظ عليها عبر إستخدام الإنترنت و/ أو تكنولوجيا المعلومات.

وعلى الرغم من عدم وجود تعريف مقبول عالمياً لجرائم الأمن السيبراني، ولكن طبقاً لدراسة Akdemir et al., (٢٠٢٠) هناك اثنان من التعريفات الأكاديمية التي تم تقديمها للجريمة السيبرانية **هما الأكثر إستخداماً في الأبحاث الأكاديمية**. التعريف الأول، هو تعريف Thomas & Loader (٢٠٠٠) وبناءً على هذا التعريف تعتبر جرائم الأمن السيبراني مجموعة من الأنشطة التي تتم من بواسطة إستخدام الكمبيوتر بشكل أساسي أو يتم تسهيلها من خلال إستخدام الكمبيوتر، وهي تعتبر إما غير قانونية أو غير مشروعة من قبل أطراف معينة، ويمكن أن يتم إجراء تلك الأنشطة من خلال الشبكات الإلكترونية العالمية. والتعريف الثاني هو تعريف Gordon & Ford (٢٠٠٦) حيث تعتبر الجريمة السيبرانية هي أي جريمة يتم تسهيلها أو ارتكابها باستخدام كمبيوتر، شبكة، أو جهاز.

وبسبب نمو تقنية الإنترنت، حصلت جرائم الأمن السيبراني على إهتمام كبير مقارنةً بالجرائم التقليدية. حيث يختلف مفهوم الجريمة السيبرانية إختلافاً كبيراً عن المفهوم التقليدي للجريمة وذلك بسبب وجود العديد من الخصائص المميزة للجرائم السيبرانية، ومن أهم هذه الخصائص:

(أ) الأشخاص ذوي المعرفة المتخصصة:

الجرائم السيبرانية هي جرائم يمكن إرتكابها فقط من خلال التكنولوجيا، لذا، من أجل إرتكاب هذا النوع من الجرائم يجب أن يكون لدى الشخص مهارات تقنية عالية،

ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب، وماهر جداً فيما يتعلق بالإنترنت وأجهزة الكمبيوتر(Puchkov, ٢٠٢٢).

(ب) الإمتداد العالمي:

في الفضاء السيبراني لا يوجد حدود، لذلك الجريمة السيبرانية هي جريمة ذات بعد دولي، أي إنها عابرة للحدود. وهذا يعني أن مرتكبي جرائم الأمن السيبراني، لديهم القدرة على ارتكاب الجرائم عن بعد والتأثير على الضحايا في أي مكان في العالم، ويعتبر هذا أحد الخصائص الرئيسية لجرائم الأمن السيبراني، مما يجعلها تختلف عن جميع أنواع الجرائم التقليدية، وأيضاً يجعلها معقدة للغاية (Furnell, ٢٠٢٠).

(ج) صعوبة جمع الأدلة:

جزء أساسي من الإبلاغ عن الجرائم هو جمع ومعالجة الأدلة الرقمية، ولكن من الصعب للغاية جمع الأدلة فيما يتعلق بالجرائم السيبرانية، ويرجع ذلك إلى أسباب عديدة على سبيل المثال، طبيعة بيانات الكمبيوتر نفسها حيث تعتبر سريعة الزوال، كذلك الإمتداد الدولي للجرائم السيبرانية وإختلاف القوانين بين الدول. وبالتالي، هناك صعوبة في التحقيق فيها، وكذلك إثباتها أمام القضاء نظراً لطبيعتها (Radoniewicz, ٢٠٢٢).

(د) حجم آثار جرائم الأمن السيبراني لا يمكن تصوره:

تعتبر جرائم الأمن السيبراني أكبر تهديد يواجه المنشأت في الوقت الحالي، وواحد من أكبر التحديات التي ستواجه البشرية وذلك على مدى العقدين المقبلين. وبالنسبة للمنشأت، فإن التكاليف والخسائر المرتبطة بالجرائم السيبرانية ضخمة إلى حد لا يمكن تخيله. حيث قد تتسبب في تلف البيانات أو سرقتها، سرقة الأموال، الملكية الفكرية، البيانات الشخصية والمالية، تعطيل أعمال الشركة بعد تعرضها لهجوم سيبراني، الإضرار بسمعة الشركة، فقدان الإنتاجية، تغيير أرقام وبيانات من السجلات المخزنة في ذاكرة الحاسبات وغير ذلك من الآثار، ويمكن أن تتسبب جرائم الأمن السيبراني في كل ذلك دون أن يكون لها أي أثر خارجي مرئي (Sviatun et .al., ٢٠٢١)

٢-٧ مفهوم ومكونات مخاطر المراجعة:

عرف معيار المراجعة المصري رقم (٢٠٠) مخاطر المراجعة بأنها خطر أن يبدي المراجع رأياً غير ملائماً، وذلك عندما تحرف القوائم المالية تحريفاً هاماً ومؤثراً. ويعتبر تخفيض مخاطر المراجعة إلى مستوى مقبول هو الإنجاز الذي يرغب المراجع في تحقيقه عند إجراء عملية المراجعة (Askary et al., ٢٠١٨). وتتكون مخاطر المراجعة من ثلاث مكونات: المخاطر الملازمة أو المتأصلة، مخاطر الرقابة، ومخاطر عدم الاكتشاف.

وتمثل **المخاطر الملازمة أو المتأصلة** إحتمالية وجود تحريف جوهري (هام ومؤثر) في أرصدة الحسابات أو في فئة من المعاملات وذلك قبل النظر في فعالية نظام الرقابة الداخلية، ويطلق على هذا الخطر مصطلح خطر الأعمال، نتيجة كونه عادةً من المخاطر المرتبطة بطبيعة النشاط الذي تمارسه منشأة الأعمال، (عبد العليم، ٢٠٢٠). وعرف معيار المراجعة المصري رقم ٢٠٠ **خطر الرقابة** بأنه هو خطر وجود تحريف هام ومؤثر (جوهري) في أرصدة الحسابات أو في فئة من المعاملات والتي قد تكون هامة (جوهرية) سواء بمفردها أو عند تجميعها مع أخطاء في أرصدة أو فئات أخرى ولا يتم منعها أو اكتشافها وتصحيحها في وقت مناسب عن طريق نظام الرقابة الداخلية. ويقصد **بمخاطر عدم الاكتشاف** بأنها خطر أن الإجراءات المنفذة من قبل المراجع لتخفيض مخاطر المراجعة إلى مستوى مقبول، لن تكتشف التحريف الموجود، الذي قد يكون هاماً ومؤثراً (جوهرياً) سواء بمفرده، أو عند تجميعه مع تحريفات أخرى، وبسبب التحريفات الهامة الغير مكتشفة، من الممكن أن يتعرض المراجع لمخاطر التقاضي، وفقدان السمعة (Agana et al., ٢٠٢٣).

٣-٧ العلاقة بين مخاطر المراجعة وجرائم الأمن السيبراني:

قد تؤثر جرائم الأمن السيبراني على تقييم المراجع الخارجي لمخاطر الرقابة والمخاطر الملازمة؛ وذلك لأن تعرض المنشأة لجرائم الأمن السيبراني قد يكون إشارة على وجود ضعف في هيكل الرقابة الداخلية المطبق والموجود في المنشأة (Chernobai et al., ٢٠١١; Benaroch et al., ٢٠١٢; Chernobai &

(Benaroch, ٢٠١٧). لذا، في حالة تعرض المنشأة لجرائم الأمن السيبراني قد يتطلب ذلك من المراجع إجراء المزيد من التخطيط لعملية المراجعة، وبالتالي، بذل المزيد من الجهد وكذلك الاختبارات للتأكد من أن هيكل الرقابة الداخلية على التقارير المالية لم يتم المساس به؛ حيث قد يتم تغيير دفاتر و سجلات الشركة، مما قد يؤدي إلى التلاعب بالقوائم المالية (Calderon & Gao, ٢٠٢٠; Rosati et al., ٢٠٢٢) وحتى إذا لم تؤثر جرائم الأمن السيبراني مباشرة على دفاتر وسجلات الشركة المحاسبية، فلايزال المراجع الخارجي مطالب ببذل المزيد من الجهد، وقد تم التأكيد على هذه المشكلة من قبل المنظمين مثل PCAOP حيث حذرت المراجعيين الخارجيين من ضرورة النظر في كيفية تأثير الحوادث الإلكترونية على هيكل الرقابة الداخلية للتقارير المالية (PCAOB, ٢٠١٠, ٢٠١٣).

وفيما يتعلق بتأثير جرائم الأمن السيبراني على مخاطر عدم الاكتشاف، فإنه يوجد علاقة سلبية بين مخاطر التحريف الهام والمؤثر (المخاطر الملازمة ومخاطر الرقابة) ومخاطر عدم الاكتشاف، بمعنى آخر، إذا قام المراجع بتقدير المخاطر الملازمة ومخاطر الرقابة عند مستوى مرتفع، يجب على المراجع تقدير مخاطر الاكتشاف عند مستوى منخفض مقبول وذلك لتخفيض خطر المراجعة إلى مستوى مقبول وتجنب فشل عملية المراجعة (Chen et al., ٢٠١٩). بالتالي، عند تقدير المراجع للمخاطر الملازمة ومخاطر الرقابة عند مستوى مرتفع نتيجة تعرض المنشأة لهجوم سيبراني، سوف يعمل المراجع على تقليل مخاطر عدم الاكتشاف وذلك من خلال إجراء اختبارات أكثر تفصيلاً، للوصول إلى مستوى مقبول لمخاطر المراجعة.

٧-٤ أتعاب المراجعة في ظل جرائم الأمن السيبراني:

تعتبر أتعاب المراجعة أحد الموضوعات الهامة في مجال المحاسبة والمراجعة، ولاتزال تحظى بإهتمام كبير من قبل الباحثين في العديد من الدراسات العلمية. وتمثل أتعاب المراجعة السعر المتفق عليه من قبل المراجع والمنشأة الخاضعة للمراجعة (عميل المراجعة) وذلك بناءً على الخدمات التي سوف تقدمها منشأة المراجعة، والتي تعكس علاقة العرض والطلب بين الطرفين. وفيما يتعلق بمفهوم أتعاب المراجعة؛ فقد تم تعريفها من قبل Choi & Yoon (٢٠١٤) بإنها عبارة عن مبلغ يحصل عليه

المراجع من عميل المراجعة، ويُحدد في ضوء الجهد المتوقع بذله لأداء عملية المراجعة ومخاطر المراجعة. ويمكن قياس الجهد المبذول وفقاً لعدد ساعات العمل المستغرقة في أداء عملية المراجعة من قبل المراجع. ويترتب على زيادة الجهد المبذول من قبل المراجع زيادة أتعاب المراجعة.

ومع تقدير المراجع للمخاطر الملازمة ومخاطر الرقابة عند مستوى مرتفع نتيجة تعرض المنشأة لهجوم سيبراني، سوف يعمل المراجع على تقليل مخاطر عدم الاكتشاف وذلك من خلال إجراء اختبارات أكثر تفصيلاً، للوصول إلى مستوى مقبول لمخاطر المراجعة. وبشكل عام، سوف يؤدي ذلك إلى أتعاب مراجعة أعلى. وأيضاً، بسبب طبيعة الهجمات السيبرانية وإحتمالية انتشار تأثيرها على نظام المعلومات المالي الخاص بالمنشأة، فمن المحتمل أنه حتى إذا قام المراجع بتقييم مخاطر الرقابة والمخاطر الملازمة عند مستوى مرتفع، لن يتمكن من اكتشاف التحريفات الجوهرية، بالتالي، قد يواجه المراجع ذلك من خلال فرض علاوة مخاطر، مما سوف يؤدي أيضاً إلى زيادة أتعاب المراجعة (متولي، غريب، ٢٠٢٢).

بينما على الجانب الاخر، قد لا تتسبب الاختراقات في أتعاب مراجعة أعلى ويمكن أن يرجع ذلك لعدة أسباب؛ **أولاً**، بما أن مخاطر الأمن السيبراني أصبحت معروفة بالفعل بالنسبة للعديد من للمراجعين الخارجيين، فإنهم يقوموا بالفعل بتضمين مخاطر الأمن السيبراني وذلك عند تحديد أتعاب المراجعة، بالتالي، في حالة تعرض المنشأة للإختراق، فإن أي زيادة في أتعاب المراجعة لن تكون جوهرية. **ثانياً**، في حالة تعرض المنشأة للإختراق يمكن التخفيف من حدة الانتهاكات وذلك من خلال آليات حوكمة الشركات (على سبيل المثال، كبار المساهمين، ولجان التكنولوجيا في مجلس الإدارة) وكذلك الرؤساء التنفيذيين والمديرين التنفيذيين والمديرين الماليين ذوي الخبرة في مجال تكنولوجيا المعلومات، مما سوف يقلل من المخاطر التي سوف يواجه المراجع، وبالتالي، قد يقلل ذلك أيضاً من زيادة أتعاب المراجعة (Smith et al., ٢٠١٩; Richardson et al., ٢٠١٩).

٧-٥ الدراسات السابقة واشتقاق فرضيات البحث:

إهتمت دراسة yen et al., (٢٠١٨) بمعرفة أثر خصائص مكتب المراجعة على أتعاب عملية المراجعة التي تلي تعرض المنشأة للإختراق، وعن طريق جمع معلومات للشركات التي تعرضت للإختراق من عام ٢٠٠٤ إلى عام ٢٠١٣، أوضحت نتائج تلك الدراسة أن أتعاب عملية المراجعة تكون أعلى في حالة حدوث جرائم تتعلق بالأمن السيبراني، حيث تكون أتعاب المراجعة أعلى حوالى ١٣,٥% في الشركات التي تعرضت للإختراق عن الشركات التي لم تتعرض إلى اختراق. ولكن اختلفت تلك النتائج في حالة كان مكتب المراجعة خبير بمجال صناعة العميل، أو يمتلك خبرة أطول مع العميل، وفي حالة كان مكتب المراجعة من الأربعة الكبار.

وهدفت دراسة Rosati et al., (٢٠١٩) إلى معرفة أثر جرائم الأمن السيبراني على مخاطر المراجعة بدلالة أتعاب مراجعة القوائم المالية، وذلك عن طريق إستخدام عينة مكونة من ٥,٦٨٧ شركة و ذلك في الفترة بين ٢٠٠٥ إلى ٢٠١٤، وأظهرت نتائج تلك الدراسة أن الشركات التي تعرضت إلى إختراق تتحمل أتعاب مراجعة أعلى بنسبة ١٢% وأيضاً الشركات في نفس صناعة المنشأت التي تعرضت للإختراق تتحمل أتعاب مراجعة أعلى من الشركات في الصناعات الأخرى. ولكن تلك الزيادة تكون فقط في العام الذي تعرضت فيه الشركة للإختراق. وأوضحت الدراسة كذلك أن المراجعين يقوموا بتضمين مخاطر الأمن السيبراني في تقييمهم لمخاطر المراجعة حتى قبل وقوع الحادث، وعندما يكون مخاطر تعرض الشركة لجرائم الأمن السيبراني مرتفعة سوف يؤدي ذلك إلى زيادة أتعاب مراجعة القوائم المالية التي يدفعها عميل المراجعة.

وعن طريق إستخدام عينة من الشركات التي تعرضت للإختراق في الفترة من ٢٠٠٥ إلى ٢٠١٨ أظهرت نتائج دراسة Richardson et al., (٢٠١٩) أنه لا يوجد اختلاف معنوي بين أتعاب مراجعة القوائم المالية للمنشأت التي تعرضت للإختراق والمنشأت التي لم تتعرض، وذلك على عكس الدراسات السابقة. وأرجعت الدراسة السبب في ذلك إلى أن مخاطر المراجعة تم تحديدها منذ وقت طويل وبالتالى تقوم منشأت المراجعة عند تحديد أتعاب المراجعة بالفعل بتضمين تلك المخاطر.

وهدفت دراسة (Ngo & Trick (٢٠٢١ إلى معرفة فيما إذا كان يركز المراجعون الخارجيون بشكل أكبر على الشركات التي تعرضت لهجمات الأمن السيبراني وذلك من خلال فرض أتعاب مراجعة أعلى. وعن طريق إستخدام أسلوب تحليل المحتوى، أظهرت نتائج الدراسة وجود علاقة إيجابية بين أتعاب المراجعة وحوادث الأمن السيبراني. وهذا يوضح أنه عند تعرض الشركة لحوادث الأمن السيبراني يجد المراجعون أن مخاطر المراجعة مرتفعة وبالتالي يبذلوا المزيد من الجهد لتقليل تلك المخاطر مما يؤدي إلى زيادة أتعاب مراجعة القوائم المالية.

وركزت دراسة (Rosati et al., (٢٠٢٢ على تحديد أثر حوادث الأمن السيبراني على جودة المراجعة. وتضمنت عينة الدراسة ٣٢٩ منشأة أمريكة تعرضت لحوادث أمن سيبراني في الفترة بين ٢٠٠٥ إلى ٢٠١٤. وتوصلت الدراسة إلى أن حوادث الأمن السيبراني لا تؤثر على جودة المراجعة، واعتمدت في ذلك على أن حوادث الأمن السيبراني قد تدل على وجود ضعف في هيكل الرقابة الداخلية الخاص بالمنشأة في تلك الحالة سوف يقوم المراجع بأداء المزيد من الاختبارات وذلك لدعم جودة المراجعة. وبناءً على الدراسات السابقة التي وجدت أن أتعاب المراجعة تزيد في حالة تعرض المنشأة لحوادث الامن السيبراني، وبما أن تلك الأتعاب يتم تحديدها بناءً على جهود عملية المراجعة، هذا يعني أن في حالة حدوث جريمة تتعلق بالأمن السيبراني سوف يزيد المراجعون من جهودهم وذلك للحفاظ على مستوى مقبول من مخاطر المراجعة، لذا، عند القيام بالمزيد من إجراءات واختبارات المراجعة، لن يتسبب ذلك في تقليل جودة المراجعة.

بعد عرض وتحليل الدراسات السابقة ذات العلاقة بموضوع البحث سواءً بشكل مباشر أو غير مباشر يمكن إستنتاج الآتي: هناك دراسات إعتبرت أن جرائم الأمن السيبراني سوف تزيد من مخاطر المراجعة، وبما أن مخاطر المراجعة = المخاطر الملازمة × مخاطر الرقابة × مخاطر عدم الاكتشاف، وفقاً لتلك الدراسات تزيد جرائم الأمن السيبراني من المخاطر الملازمة ومخاطر الرقابة، ولكي يقوم المراجع بتخفيض خطر المراجعة إلى مستوي مقبول، يعمل المراجع على تقليل مخاطر عدم الاكتشاف وذلك عن طريق إجراء المزيد من إجراءات واختبارات المراجعة، مما

يترتب عليه زيادة الجهد المبذول من قبل المراجع وبالتالي زيادة أتعاب مراجعة القوائم المالية.

وعلى الغكس من ذلك، اعتبرات دراسة Richardson et al., (٢٠١٩) أن جرائم الأمن السيبراني سوف تزيد من مخاطر المراجعة، ولكنها لن تؤثر على أتعاب مراجعة القوائم المالية، لأن المراجعين قاموا بالفعل بتضمين تلك المخاطر ضمن مخاطر المراجعة وذلك من البداية وإعتمدت تلك الدراسة على عينة أكبر من الدراسات السابقة.

وفي ضوء ما سبق يمكن اشتقاق فرضيات البحث على النحو التالي:

الفرضية الأولى (H_1): تؤثر جرائم الأمن السيبراني معنوياً وطردياً على أتعاب مراجعة القوائم المالية.

الفرضية الثانية (H_2): تؤثر جرائم الأمن السيبراني معنوياً وطردياً على مخاطر المراجعة.

الفرضية الثالثة (H_3): تؤثر مخاطر المراجعة معنوياً وطردياً على أتعاب مراجعة القوائم المالية.

الفرضية الرابعة (H_4): تؤثر جرائم الأمن السيبراني معنوياً وطردياً بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة.

٧-٦ الدراسة التطبيقية:

تهدف الدراسة التطبيقية إلى اختبار تأثير جرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية، وذلك في وجود مخاطر المراجعة كمتغير وسيط.

٧-٦-١ مجتمع وعينة الدراسة التطبيقية:

يتكون مجتمع الدراسة التطبيقية من شركات قطاع الإتصالات والإعلام وتكنولوجيا المعلومات المقيدة في البورصة المصرية، وذلك خلال الفترة الزمنية ٢٠١٧-٢٠٢٠؛ حيث يعتبر هذا القطاع هو الأكثر تعرضاً للتهديدات والجرائم

السيبرانية وذلك وفقاً للإستراتيجية الوطنية للأمن السيبراني (الرشيدي، السيد، ٢٠١٩). ويحكم اختيار الشركات التي تتضمنها عينة الدراسة خلال الفترة من ٢٠١٧ حتى ٢٠٢٠ المحددات التالية: توافر محاضر اجتماعات الجمعيات العامة وتقارير مجلس الإدارة للشركات محل الدراسة وذلك خلال سنوات الدراسة من أجل الحصول على قيمة الأتعاب السنوية للمراجع؛ توافر القوائم المالية والإيضاحات المتممة لها خلال سنوات الدراسة؛ وأن تقوم الشركات محل الدراسة بنشر قوائمها المالية بالعملة المحلية المصرية (الجنيه المصري)؛ والأ تكون الشركة قد تعرضت للشطب أو التوقف؛ وأن يكون مضى على قيدها سنة أو أكثر وذلك خلال فترة الدراسة.

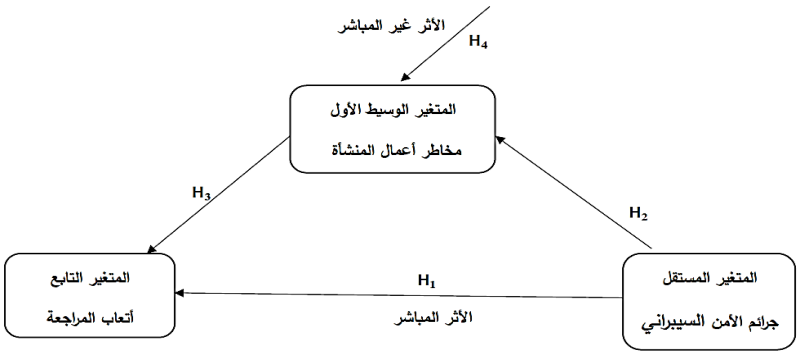
٧-٦-٢ مصادر الحصول على البيانات:

تم الحصول على البيانات المتعلقة بعينة الدراسة من خلال القوائم المالية السنوية للشركات، الإيضاحات المتممة للقوائم المالية، محاضر اجتماعات الجمعيات العامة ومجالس الإدارة، والمعلومات المتوفرة على الموقع الإلكتروني للشركة، أو ومن المعلومات المتوفرة على موقع البورصة المصرية https://egx.com.eg، وموقع مباشر مصر www.Mubasher.info. وفيما يتعلق بالبيانات حول تعرض الشركات محل الدراسة لجرائم الأمن السيبراني، فقد تم تتبع الأخبار المتعلقة بتعرض الشركات محل الدراسة لأي هجوم سيبراني وذلك بسبب ندرة الإفصاح من جانب الشركات المقيدة في البورصة المصرية عن تعرضها لأي هجوم، وتم التأكد من تعرض تلك الشركة لجرائم سيبرانية حيث تعرضت لإختراق نتيجة وجود ثغرة في نوع معين من الأجهزة الخاصة بها، وقد نتج عن هذا الهجوم تدمير هذا النوع من الأجهزة وإستبداله بجهاز آخر للعملاء.

٧-٦-٣ نموذج الدراسة وتوصيف وقياس متغيراتها:

تتكون متغيرات الدراسة من متغير تابع هو أتعاب مراجعة القوائم المالية، ومتغير مستقل هو جرائم الأمن السيبراني، ومتغير وسيط هو مخاطر المراجعة. وإستناداً إلى فرضيات الدراسة، يوضح الشكل التالي عرضاً لنموذج الدراسة ثم يليه توضيف وقياس متغيرات الدراسة:

شكل 1: نموذج الدراسة في ظل التحليل الأساسي



ويمكن توصيف وقياس متغيرات الدراسة كالتالي:

جدول(١): توصيف وقياس متغيرات الدراسة

اسم المتغير	نوع المتغير	توصيف المتغير	طريقة القياس	الأثر المتوقع على المتغير التابع
جرائم الأمن السيبراني	مستقل	أي جريمة يتم ارتكابها عبر الإنترنت وأنظمة الكمبيوتر. ويوجد مجموعة من الجرائم السيبرانية التي تؤثر على سرية وسلامة وتوافر البيانات وأنظمة الكمبيوتر؛ وهي تشمل الوصول الغير مصرح به إلى أنظمة الكمبيوتر، الإعتراض الغير شرعي لعمليات إرسال البيانات، التدخل في البيانات (إتلاف، حذف، أو تغيير البيانات)، إعاقة عمل الكمبيوتر أو أي جهاز آخر وذلك بدون وجه حق، التزوير، الإحتيال، وسرقة الهوية. ويوجد أنواع أخرى من الجرائم السيبرانية مثل الجرائم المرتبطة بالمحتوى، والمواد التي تدعو إلى عمل مرتبط بالإرهاب (Mphatheni & Malulek, ٢٠٢٢).	متغير وهمي، يأخذ (١) إذا تعرضت الشركة لجرائم الأمن السيبراني، و(صفر) إذا كان بخلاف ذلك (Rosati et al., ٢٠١٩).	+
مخاطر المراجعة	وسيط	عرف معيار المراجعة المصري رقم (٢٠٠) مخاطر المراجعة بأنها خطر أن يبدي المراجع رأياً غير ملائماً، وذلك عندما تحرف القوائم المالية تحريفاً هاماً ومؤثراً (جوهرياً).	أتعاب المراجعة الغير عادية قياساً على (Choi et al., ٢٠١٠).	+

أتعاب المراجعة	تابع	هي عبارة عن مبلغ يحصل عليه المراجع من عميل المراجعة، ويُحدد في ضوء الجهد المتوقع بذله لأداء عملية المراجعة ومخاطر المراجعة. ويمكن قياس الجهد المتوقع بذله وفقاً لعدد ساعات العمل المستغرقة في أداء عملية المراجعة من قبل المراجع. ويترتب على زيادة الجهد المبذول من قبل المراجع زيادة أتعاب المراجعة (Choi & Yoon, ٢٠١٤).	اللوغاريتم الطبيعي لأتعاب المراجعة، قياساً على (Rosati et al., ٢٠١٩).	

٤-٦-٧ المتغيرات الرقابية:

تتضمن المتغيرات الرقابية مجموعة من المتغيرات التي قد تكون ذات تأثير محتمل على المتغير التابع (أتعاب مراجعة القوائم المالية)، وسوف يتم تضمينها من أجل تحديد أتعاب المراجعة المقدرة. ويمكن توصيف قياس المتغيرات الرقابية كالتالي:

جدول(٢): توصيف وقياس المتغيرات الرقابية

اسم المتغير	توصيف المتغير	طريقة القياس	الأثر المتوقع على المتغير التابع
مخاطر أعمال المنشأة	خطر أن الحالة الإقتصادية للعميل ستتدهور إما على المدى القصير أو الطويل (Johnstone, ٢٠٠٠).	نسبة الرافعة المالية (Suryani & Sitorus, ٢٠١٨).	+
حجم منشأة عميل المراجعة	يعد أحد الخصائص المميزة التي يتم الإستناد إليها وذلك عند تحديد أتعاب المراجعة، وهي تشير إلى قدرة المنشأة على توليد الإيرادات من خلال أنشطتها، وذلك بالإعتماد على طاقة وإمكانيات المنشأة المادية والبشرية والتكنولوجية وإجمالي حجم أصولها (Coffie & Bedi, ٢٠١٩؛).	اللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام (Coffie & Bedi, ٢٠١٩).	+
حجم مكتب المراجعة	يُشير حجم مكتب المراجعة إلى الإمكانيات المادية، البشرية، التكنولوجية والمهنية التي تساعد المراجع على أداء مجموعة واسعة من الخدمات المهنية ذات الجودة، لعدد أكبر من العملاء يمثلون حصة كبيرة في السوق (عبد الرحيم، محمد ٢٠٢٢). وقد يكون مكتب المراجعة الذي يراجع القوائم المالية لعميل المراجعة من الأربعة الكبار Big٤، أو أي مكتب آخر.	متغير وهمي، يأخذ (١) إذا كان مكتب المراجعة من الأربعة الكبار Big؛، و(صفر) إذا كان بخلاف ذلك (Hay et al., ٢٠٠٦).	+
ربحية منشأة عميل المراجعة	وهي تعني قدرة المنشأة على الإستخدام الفعال للموارد المخصصة لها (عبد الرحيم محمد، ٢٠٢٢).	معدل العائد على الأصول، قياساً على (متولي، غريب، ٢٠٢٢).	+ أو -

التخصص الصناعي لمكتب المراجعة	يعتبر التخصص الصناعي لمكتب المراجعة أحد الاستراتيجيات التنافسية التي تؤدي إلى خلق ميزة تنافسية لمكتب المراجعة وذلك من خلال تركيزه على مراجعة صناعة محددة. فمن خلال التخصص في صناعة محددة، يكتسب مكتب المراجعة المعرفة والخبرة التي تمكنه من تحسين الحكم المهني وفعالية عملية المراجعة وبالتالي تقديم خدمة مميزة، تمكنه من بناء سمعته وزيادة حصته في السوق (بدوي، ٢٠١٨ ؛ Agana et al., ٢٠٢٣).	مدخل الحصة السوقية على أساس عدد العملاء قياساً على (Ahmed et al., ٢٠١٦).	+ أو -
درجة تعقد عمليات منشأة عميل المراجعة	وهي تشير إلى مدى صعوبة تتبع عمليات وأنشطة منشأة عميل المراجعة، وقد يكون ذلك بسبب كثرة الفروع أو الشركات لعميل المراجعة، تنوع وتعقد عمليات عميل المراجعة. وقد يتم قياسها من خلال اللوغاريتم الطبيعي لإجمالي المخزون والعملاء، أو اللوغاريتم الطبيعي لعدد الفروع أو الشركات التابعة لعميل المراجعة (عبد الرحيم، محمد، ٢٠٢٢).	اللوغاريتم الطبيعي لإجمالي المخزون والعملاء قياساً على (Kraub et al., ٢٠١٥).	+
تأخر تقرير المراجعة	هي الفترة التي يحتاج إليها المراجع الخارجي من أجل إستكمال عملية مراجعة القوائم المالية للشركة وذلك من تاريخ نهاية السنة المالية لعميل المراجعة (Abdillah, ٢٠١٩).	عدد الأيام المنقضية من تاريخ نهاية السنة المالية لعميل المراجعة، وحتى تاريخ توقيع المراجع على تقرير المراجعة (Abdillah, ٢٠١٩).	+

٧-٦-٥ اختبار فرضيات البحث:

وفيما يلي سوف يتم إختبار فرضيات البحث:

٧-٦-٥-١ اختبار الفرضية الأولى

تهدف الفرضية الأولى للبحث تحديد تأثير جرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية السنوية. ولاختبار هذه الفرضية سوف يتم إجراء تحليل الانحدار البسيط وذلك وفقاً للمعادلة الآتية:

$$LAF_{it} = \beta_0 + \beta_1 CI_{it} + \varepsilon_{it} \quad (1)$$

- حيث أن:

LAF_{it}: اللوغاريتم الطبيعي لأتعاب المراجعة للمنشأة (i)وذلك في السنة (t).

β_0: قيمة الثابت في معادلة الانحدار.

β_1: معامل الانحدار لتعرض الشركة لجريمة سيبرانية، وكذلك يحدد اتجاه العلاقة بين المتغيرين.

CI_{it}: تمثل تعرض المنشأة (i) لجريمة سيبرانية وذلك في السنة (t).

ε_{it}: تمثل الخطأ العشوائي لنموذج الانحدار البسيط.

ويظهر الجدول التالي نتائج التحليل الإحصائي الخاصة باختبار الفرضية الأولى.

جدول(٣): نتائج اختبار الفرضية الأولى (H_1)

المتغيرات	معاملات الانحدار المقدرة (β)	اختبار T	
		القيمة	مستوى المعنوية
الحد الثابت (Constant)	٥,٤٩١	٥٥,٤٣٢	.٠٠٠
CI	.٨٣٧	٢,٩٨٨	.٠١٠
معامل التحديد (R^2): ٣٨٩. معامل التحديد المعدل (Adjusted R^2): ٣٤٦. قيمة اختبار ف (F): ٨,٩٢٨ المعنوية (.Sig): ٠١٠.			

بقراءة الجدول السابق يتضح الآتي:

- معنوية نموذج الانحدار حيث بلغت قيمة (F) ٨,٩٢٨ والتي جاءت دالة إحصائياً عند مستوى معنوية (٠١٠.) وهي أقل من المستوى المعنوي المقبول ٥٪، وبالتالي فإن المتغير المستقل (جرائم الأمن السيبراني) يؤثر معنوياً على المتغير التابع (أتعاب مراجعة القوائم المالية).
- قيمة معامل التحديد(R^2) تساوي (٣٨٩.) وهذا يعني أن المتغير المستقل (جرائم الأمن السيبراني) يفسر٣٨,٩% من التغيرات التي حدثت في المتغير التابع (أتعاب مراجعة القوائم المالية). وباقي النسبة ترجع إلى الخطأ العشوائي في التقدير والمتغيرات الأخرى التي لا يتضمنها النموذج.

- تعبر الإشارة الموجبة لمعامل الانحدار (٨٣٧.) عن أن العلاقة بين هذين المتغيرين هي علاقة طردية. وهذا يعني أنه مع تعرض المنشأة لجرائم الأمن السيبراني سوف يؤدي ذلك إلى زيادة أتعاب المراجعة.

وبناءً على ما سبق، فإنه **يتم قبول الفرضية الأولى (H١)، التي تنص على أنه "تؤثر جرائم الأمن السيبراني معنوياً وطردياً على أتعاب مراجعة القوائم المالية"**. وتتفق هذه النتيجة مع ما توصلت إليه بعض الدراسات مثل (Smith et al., ٢٠١٨; Rosati et al., ٢٠١٩; Li et al., ٢٠٢٠). ويعتبر ذلك أمر منطقياً، فمن المتوقع مع تعرض المنشأة لهجوم سيبراني، أن يتطلب ذلك من المراجع إجراء المزيد من التخطيط لعملية المراجعة، وبالتالي، بذل المزيد من الجهد وكذلك الاختبارات للتأكد من أن هيكل الرقابة الداخلية على التقارير المالية لم يتم المساس به؛ حيث قد يتم تغيير دفاتر و سجلات الشركة، مما قد يؤدي إلى التلاعب بالقوائم المالية. وحتى إذا لم تؤثر جرائم الأمن السيبراني مباشرة على دفاتر وسجلات الشركة المحاسبية، فلايزال المراجع الخارجي مطالب ببذل المزيد من الجهد، وقد تم التأكيد على هذه المشكلة من قبل المنظمين مثل PCAOP حيث حذرت المراجعيين الخارجيين من ضرورة النظر في كيفية تأثير الحوادث الإلكترونية على هيكل الرقابة الداخلية للتقارير المالية (PCAOB, ٢٠١٠, ٢٠١٣).

٧-٦-٥-٢ اختبار الفرضية الثانية للبحث:

تهدف الفرضية الثانية للبحث تحديد تأثير جرائم الأمن السيبراني على مخاطر المراجعة، وسوف يتم قياس مخاطر المراجعة من خلال **أتعاب المراجعة غير العادية**. ويتم اختبار هذه الفرضية من خلال الاعتماد على **A two-stage approach**. لذا، **أولاً**، سوف يتم تقدير أتعاب المراجعة العادية من خلال النموذج (٢). **ثانياً**، سوف يتم قياس أتعاب المراجعة غير العادية من خلال الفرق بين أتعاب المراجعة الفعلية المدفوعة **(LAF)** وأتعاب المراجعة التي تم تقديرها من خلال النموذج ٢ (Choi et al., ٢٠١٠). وفي النموذج (٢) تم إستخدام مجموعة من المحددات التي قد تؤثر على أتعاب المراجعة وذلك في ضوء الدراسات السابقة مثل (عبد الرحيم، محمد، ٢٠٢٢؛ طلخان، ٢٠٢٢؛ Choi et al., ٢٠١٠; Blankley et al., ٢٠١٢; Janaturi &

Wiryaningrum, ٢٠١٨; Kanakriyah, ٢٠٢٠; Amran et al., ٢٠٢١; Saleh & Magdi, ٢٠٢٣). لذا، من أجل اختبار هذه الفرضية سوف يتم أولاً، إجراء تحليل الانحدار المتعدد ، وذلك وفقاً للمعادلة الآتية:

$$LAF_{it} = \beta_0 + \beta_1 LEV_{it} + \beta_2 LNTA_{it} + \beta_3 Big4_{it} + \beta_4 ROA_{it} + \beta_5 SPEC_{it} + \beta_6 LNINVER_{it} + \beta_7 ARL_{it} + \beta_8 LOSS_{it} + \varepsilon_{it} + (٢)$$

- حيث أن:

LEV_{it}: نسبة الرافعة المالية للمنشأة (i) في السنة (t). وهي عبارة عن إجمالي الإلتزامات/ إجمالي الأصول؛

$LNTA_{it}$: اللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام للمنشأة (i) في السنة (t)؛

$Big4_{it}$: متغير وهمي، يأخذ (١) إذا كان مكتب المراجعة من الأربعة الكبار Big٤ ، و (صفر) إذا كان بخلاف ذلك، وذلك للمكتب (i) في السنة (t)؛

$SPEC_{it}$: التخصص الصناعي لمنشأة المراجعة. وهو عبارة عن عدد عملاء مكتب المراجعة/ إجمالي عدد العملاء في الصناعة؛

ROA_{it}: معدل العائد على الأصول للمنشأة (i) في السنة (t). ويقاس بنسبة صافي الدخل قبل الضرائب إلي إجمالي الأصول؛

$LNINVREC_{it}$: اللوغاريتم الطبيعي لإجمالي المخزون والعملاء للمنشأة (i) في السنة (t)؛

ARL_{it} : عدد الأيام المنقضية من تاريخ نهاية السنة المالية لعميل المراجعة، وحتى تاريخ توقيع المراجع على تقرير المراجعة؛

LOSS: متغير وهمي، بحيث يأخذ القيمة ١ في حالة عانت المنشأة من صافي خسارة، بينما يأخذ القيمة ٠ فيما عدا ذلك.

ويظهر الجدول التالي نتائج التحليل الإحصائي الخاصة بنموذج أتعاب المراجعة العادية.

جدول (٤): نتائج تشغيل نموذج أتعاب المراجعة العادية

المتغيرات	معامل الانحدار(β)	اختبار T	
		القيمة	مستوى المعنوية
الحد الثابت (Constant)	-٢,٦٥١	-٤,٨٧٠	.٠٠٢
LEV	.٥٩٤	٢,٤٧٥	.٠٤٣
LNTA	١,٥٩٧	٩,٩٦٨	.٠٠٠
Big٤	١,٣٧٧	١٩,١٦٨	.٠٠٠
ROA	-.٥٧٤	-٢,٢٤٦	.٠٦٠
SPEC	-١١,٠٨٤	-١١,٨١٦	.٠٠٠
LNINVREC	-.٠٢٢	.١٢٢	.٩١٤
ARL	.٠٠٥	٢,٣٨٢	.٠٤٩
LOSS	.٠٤٩	.٤٦٥	.٦٦٢
معامل التحديد (R^2): ٩٩٧.			
معامل التحديد المعدل (Adjusted R^2): ٩٩٤.			
قيمة اختبار ف (F): ٣١٧,٨٧٥			
المعنوية (.Sig): ٠٠٠.			

وبعد تقدير أتعاب المراجعة، سوف يتم إستخدام بواقي نموذج أتعاب المراجعة (Residuals)، كمقياس للأتعاب غير العادية لعملية المراجعة مع إهمال إشارة تلك البواقي، حيث تمثل تلك البواقي الفرق بين **أتعاب المراجعة الفعلية المدفوعة – أتعاب المراجعة المقدرة وفقاً للنموذج ٢**، ثم إدراجها كمتغير تابع في نموذج الانحدار التالي وذلك لتحديد تأثير جرائم الأمن السيبراني على مخاطر المراجعة:

$$\mathbf{ABAFEE_{it} = \beta_0 + \beta_1 CI_{it} + \varepsilon_{it} \quad (٣)}$$

حيث تعبر **ABAFEE** عن الأتعاب غير العادية لعملية المراجعة (i) وذلك في السنة (t) والتي تم تقديرها من النموذج ٤. وباقي المتغيرات كما سبق توضيحها. ويظهر الجدول التالي نتائج التحليل الإحصائي الخاصة باختبار الفرضية الثانية للبحث.

جدول(٥): نتائج اختبار الفرضية الثانية (H_2)

المتغيرات	معامل الانحدار(β)	اختبار T	
		القيمة	مستوى المعنوية
الحد الثابت (Constant)	.٠١٤	٢,٣٥٨	.٠٣٣
CI	.٠٤٦	٢,٧٤٦	.٠١٦
معامل التحديد (R^2): ٣٥.			
معامل التحديد المعدل (Adjusted R^2): ٣٠٤.			
قيمة اختبار ف (F): ٧,٥٣٨			
المعنوية (.Sig): ٠١٦.			

بقراءة الجدول السابق يتضح الآتي:

- معنوية نموذج الانحدار حيث بلغت قيمة (F) ٧,٥٣٨ والتي جاءت دالة إحصائياً عند مستوى معنوية (٠١٦.) وهي أقل من المستوى المعنوي المقبول ٥٪، وبالتالي فإن المتغير المستقل (جرائم الأمن السيبراني) يؤثر معنوياً على المتغير التابع (مخاطر المراجعة).
- قيمة معامل التحديد(R^2) تساوي (٣٥.) وهذا يعني أن المتغير المستقل (جرائم الأمن السيبراني) يفسر٣٥ % من التغيرات التي حدثت في المتغير التابع (مخاطر المراجعة). وباقي النسبة ترجع إلى الخطأ العشوائي في التقدير والمتغيرات الأخرى التي لا يتضمنها النموذج.
- تعبر الإشارة الموجبة لمعامل الانحدار (٠٤٦.) عن أن العلاقة بين هذين المتغيرين هي علاقة طردية.

وبناءً على ما سبق، فإنه **يتم قبول الفرضية الثانية للبحث (H_2)، التي تنص على أنه "تؤثر جرائم الأمن السيبراني معنوياً وطردياً على مخاطر المراجعة".**

٧-٦-٥-٣ اختبار الفرضية الثالثة للبحث:

تهدف الفرضية الثالثة للبحث تحديد تأثير مخاطر المراجعة على أتعاب مراجعة القوائم المالية، وذلك في ظل وجود جرائم الأمن السيبراني كمتغير مفسر آخر ولاختبار هذه الفرضية سوف يتم إجراء تحليل الانحدار المتعدد، بناءً على المعادلة الآتية:

$$LAF_{it} = \beta_0 + \beta_1 ABAFF_{it} + \beta_2 CI_{it} \quad (٤)$$

ويظهر الجدول التالي نتائج التحليل الإحصائي الخاصة باختبار الفرضية الثالثة.

جدول (٦) نتائج اختبار الفرضية الثالثة (H٣)

المتغيرات	معامل الانحدار(β)	اختبار T	
		القيمة	مستوى المعنوية
الحد الثابت (Constant)	٥,٣٦٧	٥٢,١٣٩	.٠٠٠
ABAFF	٨,٨٨٢	٢,٢٦٢	.٠٤١
CI	.٤٢٨	١,٤٠٢	.١٨٤
معامل التحديد (R^2): ٥٦٢.			
معامل التحديد المعدل (Adjusted R^2): ٤٩٤.			
قيمة اختبار ف (F): ٨,٣٣٤			
المعنوية (.Sig): ٠٠٠.			

بقراءة الجدول السابق يتضح الآتي:

- معنوية نموذج الانحدار المتعدد حيث بلغت قيمة (F) ٨,٣٣٤ والتي جاءت دالة إحصائياً عند مستوى معنوية (٠٠٠.) وهي أقل من المستوى المعنوي المقبول ٥٪.
- وبلغت قيمة معامل التحديد ٥٦٢. وهذا يعني أن المتغيرات المتضمنة في نموذج الانحدار المتعدد تفسر ٥٦,٢٪ من التغيرات في المتغير التابع (أتعاب المراجعة).

وبفحص نتائج اختبار T-Test لاختبار معنوية كل متغير على حدة يتضح الآتي:

- توجد علاقة معنوية بين أتعاب مراجعة القوائم المالية ومخاطر المراجعة، حيث أن قيمة مستوى المعنوية أقل من ٥٪. وتعبر الإشارة الموجبة لمعامل الإنحدار أن العلاقة بين المتغيرين هي علاقة طردية.
- لا توجد علاقة معنوية بين أتعاب مراجعة القوائم المالية وجرائم الأمن السيبراني، حيث أن قيمة مستوى المعنوية أقل من ٥٪.

٧-٦-٥-٤ اختبار الفرضية الرابعة للبحث:

تهدف الفرضية الرابعة للبحث اختبار التأثير غير المباشر لجرائم الأمن السيبراني على أتعاب مراجعة القوائم المالية، وذلك من خلال جعل مخاطر المراجعة متغير

وسيط، ولتحقيق ذلك كان يجب التحقق أولاً من مدى إمكانية أن تكون مخاطر المراجعة متغير وسيط أم لا، وتم ذلك عن طريق الاعتماد على طريقة Kenny & Baron (١٩٨٦) والتي تعتبر واحدة من أكثر الطرق إستخداماً (Otuya, ٢٠١٩). وطبقاً لتلك الطريقة، يجب أن تتحقق **ثلاثة شروط** أولاً حتى نقول أن المتغير الوسط يتوسط العلاقة بين المتغير المستقل والتابع وهما كالتالي:

أ) يجب أن يؤثر المتغير المستقل (جرائم الأمن السيبراني) تأثيراً معنوياً على المتغير التابع (أتعاب المراجعة)، وذلك تم اختباره وتحققه في الفرضية الأولى، وبلغ مستوى المعنوية ٠١٠. وهي أقل من مستوى المعنوية المقبول ٥٪.

ب) يجب أن يؤثر المتغير المستقل (جرائم الأمن السيبراني) تأثيراً معنوياً على المتغير الوسيط (مخاطر المراجعة)، وذلك تم اختباره في الفرضية الثانية، وتحقق يتحقق هذا الشرط حيث بلغ مستوى المعنوية ٠١٦. وهي أقل من مستوى المعنوية المقبول ٥٪.

ج) يجب أن يؤثر المتغير الوسيط (مخاطر المراجعة) تأثيراً معنوياً على المتغير التابع (أتعاب المراجعة) وذلك بوجود المتغير المستقل جرائم الأمن السيبراني كمتغير مفسر آخر، وقد تم اختباره في الفرضية الثالثة، وتحقق هذا الشرط حيث بلغ مستوى المعنوية لمخاطر المراجعة ٠٤١. وهي أقل من مستوى المعنوية المقبول ٥٪.

وبناءً على ما سبق ونظراً لتحقق الشروط الثلاثة، فهذا يشير إلى أن مخاطر المراجعة تصلح أن تكون متغير وسيط بمعنى أن تتوسط العلاقة بين جرائم الأمن السيبراني وأتعاب المراجعة. ولتحديد نوع الوساطة سوف يتم إجراء مقارنة بين نتائج الفرضية الأولى والفرضية الثالثة.

جدول (٧) ملخص نتائج تحليل العلاقة بين المتغير المستقل والتابع بعد إضافة متغير مخاطر المراجعة كمتغير وسيط

المتغيرات	نموذج (١) العلاقة بدون متغير وسيط		نموذج (٤) العلاقة مع إستخدام المتغير الوسيط	
	معامل الانحدار	Sig	معامل الانحدار	Sig
الحد الثابت	٥,٤٩١	.٠٠٠	٥,٣٦٧	.٠٠٠
CI	.٨٣٧	.٠١٠	.٤٢٨	.١٨٤
ABAFEE	.....	.....	٨,٨٨٢	.٠٤١
معامل التحديد R^2	.٣٨٩		.٥٦٢	

وبقراءة الجدول السابق يتضح الآتي:

- يوجد علاقة معنوية بين المتغير المستقل (جرائم الأمن السيبراني) والمتغير التابع (أتعاب المراجعة)، **وذلك بدون وجود المتغير الوسيط.** وبلغت قيمة معامل الانحدار (.٨٣٧)، وهذا يدل على أن العلاقة بين المتغيرين هي علاقة طردية، وبلغت قيمة معامل التحديد(R^2) (.٣٨٩)، أي أن النموذج يفسر ٣٨,٩% من التغيرات في المتغير التابع.

- وبإدخال متغير "مخاطر المراجعة" كمتغير وسيط للعلاقة بين المتغير المستقل والتابع، **في ظل وجوده أصبحت جرائم الأمن السيبراني لا تؤثر معنوياً على أتعاب المراجع**ة، حيث أصبح مستوى المعنوية (.١٨٤) وهي أكبر من مستوى المعنوية المقبولة ٥٪. وأيضاً ارتفعت قيمة معامل التحديد (R^2) إلى (.٥٦٢) أي أن النموذج يفسر ٥٦,٢٪ من التغيرات في المتغير التابع.

وبناءً على ما سبق، يعتبر نوع الوساطة هو **وساطة كاملة أو كلية** حيث لم يعد المتغير المستقل يؤثر على المتغير التابع عند وجود المتغير الوسيط. وبالتالي، يتم **قبول الفرضية الرابعة**، التي تنص على أنه "تؤثر جرائم الأمن السيبراني معنوياً وطردياً بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة".

٨- ملخص نتائج اختبار فرضيات البحث:

ويظهر الجدول التالي ملخص نتائج اختبار فرضيات البحث.

جدول (٨) : ملخص نتائج اختبار فرضيات البحث

الفرضيات	النص	النتائج
(H_1)	تؤثر جرائم الأمن السيبراني معنوياً وطردياً على أتعاب مراجعة القوائم المالية.	**قبول**
(H_2)	تؤثر جرائم الأمن السيبراني معنوياً وطردياً على مخاطر المراجعة.	**قبول**
(H_3)	تؤثر مخاطر المراجعة معنوياً وطردياً على أتعاب مراجعة القوائم المالية.	**قبول**
(H_4)	تؤثر جرائم الأمن السيبراني معنوياً وطردياً بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة.	**قبول**

٩- نتائج وتوصيات البحث:

توصل البحث إلى عدة نتائج، أهمها ما يلي:

- تؤثر جرائم الأمن السيبراني تأثيراً معنوياًو طردياً على أتعاب مراجعة القوائم المالية، وهو ما يؤدي إلى **قبول الفرضية الأولى للبحث،** التي تنص على أنه "تؤثر جرائم الأمن السيبراني معنوياً وطردياً على أتعاب مراجعة القوائم المالية". وتتفق هذه النتيجة مع ما توصلت إليه بعض الدراسات مثل (Smith et al., ٢٠١٨; Rosati et al., ٢٠١٩; Li et al., ٢٠٢٠).

- تؤثر جرائم الأمن السيبراني معنوياً وطرديا على مخاطر المراجعة. ويؤدي ذلك إلى **قبول الفرضية الثانية للبحث،** التي تنص على أنه "تؤثر جرائم الأمن السيبراني معنوياً وطردياً على مخاطر المراجعة".

- تؤثر مخاطر المراجعة معنوياً وطردياً على أتعاب مراجعة القوائم المالية. ويؤدي ذلك إلى **قبول الفرضية الثالثة للبحث،** التي تنص على أنه تؤثر مخاطر المراجعة معنوياً وطردياً على أتعاب مراجعة القوائم المالية.

- تؤثر جرائم الأمن السيبراني تأثيراً معنوياً وطردياً بشكل غير مباشر على أتعاب مراجعة القوائم المالية من خلال مخاطر المراجعة. ويؤدي ذلك إلى **قبول الفرضية الرابعة للبحث،** ويعتبر ذلك أمراً منطقياً فمع تقدير المراجع للمخاطر الملازمة ومخاطر الرقابة عند مستوى مرتفع نتيجة تعرض المنشأة لهجوم سيبراني، سوف يعمل المراجع على تقليل مخاطر عدم الاكتشاف وذلك من خلال إجراء اختبارات أكثر تفصيلاً، للوصول إلى مستوى مقبول لمخاطر المراجعة. وبشكل عام، سوف يؤدي ذلك إلى أتعاب مراجعة أعلى. وأيضاً، بسبب طبيعة الهجمات السيبرانية وإحتمالية انتشار تأثيرها على نظام المعلومات المالي الخاص بالمنشأة، فمن المحتمل أنه حتى إذا قام المراجع بتقييم مخاطر الرقابة والمخاطر الملازمة عند مستوى مرتفع، لن يتمكن من اكتشاف التحريفات الجوهرية، بالتالي، قد يواجه المراجع ذلك من خلال فرض علاوة مخاطر، مما سوف يؤدي أيضاً إلى زيادة أتعاب المراجعة.

وبشأن توصيات البحث، فإن أهمها ما يلي:

- على الشركات المصرية أن تعمل على تطوير الأمن السيبراني، وقد يتم ذلك من خلال إنشاء لجنة متخصصة في الأمن السيبراني، تحديد مبالغ من أجل الإنفاق على دعم وتطوير الأمن السيبراني، وتوفير دورات إلزامية لتنمية وتطوير مهارات الموظفين فيما يتعلق بكيفية التعامل مع مخاطر الأمن السيبراني.

- العمل على تشجيع الشركات المصرية المقيدة بالبورصة المصرية بالإفصاح عن مخاطر الأمن السيبراني وكيفية إدارتها. حيث يعتبر الإفصاح عن مخاطر الأمن السيبراني اختيارياً في مصر، ولا توجد أية متطلبات من سوق الأوراق المالية المصرية للشركات المقيدة بتقديم هذا النوع من الإفصاح

- العمل على وضع مشرع قانون يلزم الشركات المصرية المقيدة بالبورصة المصرية بالإبلاغ والإفصاح عن أي هجمات سيبرانية تتعرض لها للمركز الوطني للإستعداد لطوارئ الحاسبات والشبكات.

- العمل على إصدار دليلاً إسترشادياً للأمن السيبراني والمخاطر المتعلقة به، وذلك من خلال التنسيق بين الجهاز المركزي للمحاسبات وجمعية المحاسبين والمراجعين المصرية لوضع دليلاً إسترشادياً يوضح كيف يجب أن يتعامل المراجع الخارجي مع الأمن السيبراني للمنشأة والمخاطر المتعلقة به. وإجراء دورات مكثفة من قبل جمعية المحاسبين والمراجعين المصرية للمراجعين الخارجيين بهدف شرح كيفية تطبيق هذا الدليل الإسترشادي، ثم إجراء اختبار بصفة دورية للمحاسبين والمراجعين المصريين يتضمن حالات عملية لمنشأت تعرضت لهجمات سيبرانية.

- الإهتمام بتدريس المقررات الدراسية التي تتعلق بالأمن السيبراني، وذلك من خلال إضافة المقررات الدراسية التي تتعلق بالأمن السيبراني، وجعلها متطلب أساسي للحصول على درجة البكالوريوس في الجامعات المصرية ويمكن إستثناء الكليات المتخصصة. وأيضاً تشجيع الباحثين على إجراء المزيد من الأبحاث في مجال الأمن السيبراني، وذلك من خلال إجراء مسابقات دورية لمكافأة الأبحاث المميزة في هذا المجال.

المراجع

أولاً المراجع باللغة العربية:

- بدوي، هبة. (٢٠١٨). أثر خطري المراجعة وأعمال عميل المراجعة على قرار مراقب الحسابات بشأن قبول التكليف بمراجعة الحسابات: دراسة تجريبية. ***مجلة الإسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة، كلية التجارة، جامعة الإسكندرية ٢(١)، ٣١١-٣٧٢.

- الرشيدي، السيد. (٢٠١٩). أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول دراسة مقارنة في قطاع تكنولوجيا المعلومات. ***مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية***، قسم المحاسبة، كلية التجارة، جامعة بني سويف، (٢)،٤٣٩-٤٨٧.

- السرحان، سالم.(٢٠٢٠). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الاردنية [رسالة ماجستير،جامعة آل البيت]. كلية الاقتصاد والعلوم الإدارية، الأردن.

- طلخان، السيدة. (٢٠٢٢). أثر قابلية التقارير المالية للقراءة ومراحل دورة حياة الشركة على أتعاب المراجعة دراسة تطبيقية على الشركات غير المالية المقيدة بالبورصة المصرية. ***مجلة الإسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة، كلية التجارة، جامعة الإسكندرية ٦(٣)، ٤٤١-٥١٣.

- عبد الرحيم، رضا، محمد، عمرو.(٢٠٢٢). دراسة واختبار تأثير خصائص منشاتي مراقب الحسابات وعميله علي أتعاب مراجعة القوائم المالية للشركات غير المالية المقيدة بالبورصة المصرية. ***المجلة العلمية للبحوث التجارية***، كلية التجارة، جامعة المنوفية،٤١ (٤)، ١٧٣-٢٢٤.

- عبد العليم، صافيناز. (٢٠٢٠). أثر مدخل المراجعة الثنائية والمراجعة المشتركة على مخاطر المراجعة. ***مجلة الدراسات المالية والتجارية***، كلية التجارة، جامعة بني سويف، ٣٠(٢)، ٤٨-٧٣.

- متولي، غريب، غريب، حسين. (٢٠٢٢). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية دراسة تطبيقية. ***المجلة العلمية للدراسات المحاسبية***، كلية التجارة، جامعة بني سويف، ٤(٤)، ٢٤٥-٣٢٨.

- هيئة الأتصالات وتقنية المعلومات السعودية. (٢٠٢٠). إجراءات التعامل مع حوادث الأمن السيبراني في قطاع الأتصالات وتقنية المعلومات والبريد.

- وزارة الاستثمار. (٢٠٠٨). المعايير المصرية للمراجعة والفحص المحدود ومهام التأكد الأخرى. معيار المراجعة المصري رقم (٢٠٠)، "الهدف من عملية مراجعة قوائم مالية والمبادئ العامة التي تحكمها".

ثانياً المراجع باللغة الإنجليزية:

- Abdillah, M., Mardijuwono, A., & Habiburrochman, H. (٢٠١٩). The effect of company characteristics and auditor characteristics to audit report lag. ***Asian Journal of Accounting,*** ٤(١), ١٢٩-١٤٤.

- Agana, J., Alon, A., & Zamore, S. (٢٠٢٣). Self-regulation versus government oversight: audit fees research. ***Journal of Accounting Literature***, Vol. ahead-of-print No. ahead-of-print.

- Ahmed, M., Hamidah, M., & Nelson, S. (٢٠١٦). The association between industry specialist auditor and financial reporting timeliness- Post MFRS period. ***Procedia Social and Behavioral Sciences***, ٢١٩, ٥٥-٦٢.

- Akdemir, N., Sungur, B., & Basaranel, B.U. (٢٠٢٠). Examining the Challenges of Policing Economic Cybercrime in the UK. ***Sayı International Security Congress,*** ١١٣, ١١٣–١٣٤.

- Amran, A., Susanto, E., Kalsum, U., Fitrianti, F., & Muslim, M. (٢٠٢١). The Effect of Company Complexity and Company Size against Audit Fees. ***Point of View Research Accounting and Auditing***, ٢(١), ٥٩-٦٥.

- Askary, S., Arnaout, J., & Abughazaleh, N. (٢٠١٨). Audit evidences and modelling audit risk using goal programming. ***International Journal of Applied Decision Sciences***, ١١(١), ١٨-٣٥.

- Benaroch, M., & Chernobai, A., & Goldstein, J. (٢٠١٢). An internal control perspective on the market value consequences of IT operational risk events. ***International Journal of Accounting Information Systems***, ١٣(٤), ٣٥٧-٣٨١.

- Benaroch, M., & Chernobai, A. (٢٠١٧). Operational IT failures, IT value destruction, and board-level IT governance changes. ***MIS Quarterly: Management Information Systems,*** ٤١(٣), ٧٢٩-٧٦٢.

- Bianchi, D., & Tosun, O. K. (٢٠١٩). Cyber-attacks and stock market activity. WBS Finance Group Research Paper No. ٢٥١.

- Blankley, A. I., D. N. Hurtt, and J. E. MacGregor. ٢٠١٢. Abnormal audit fees and restatement. *Auditing: A Journal of Practice & Theory,* ٣١(١), ٧٩-٩٦.

- Calderon, T., & Gao, L. (٢٠٢٠). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. ***International Journal of Auditing,*** ٢٥(١), ٢٤-٣٩.

- Cavusoglu, H., Mishra, B., and Raghunathan, S. (٢٠٠٤). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. ***International Journal of Electronic Commerce,*** ٩(١), ٧٠-١٠٤.

- Chen, H., Hua, S., Liu, Z., & Zhang, M. (٢٠١٩). Audit fees, perceived audit risk, and the financial crisis of ٢٠٠٨. ***Asian Review of Accounting,*** ٢٧(١), ٩٧-١١١.

- Chernobai, A., Jorion, P., & Yu, F. (٢٠١١). The determinants of operational risk in US financial situations. ***Journal of Financial and Quantitative Analysis***, ٤٦(٦), ١٦٨٣-١٧٢٥.

- Choi, J., KIM, J., & ZANG, Y. (٢٠١٠). Do Abnormally High Audit Fees Impair Audit Quality? ***Auditing: A Journal of Practice and Theory***, ٢٩(٢), ١١٥-١٤٠.

- Choi, W. and Yoon, S. (٢٠١٤). Effects of IFRS adoption, big N factor and the IFRS-related consulting services of auditors on audit fees: the case of Korea. ***Asian Journal of Business and Accounting,*** ٧ (١), ٥٥-٧٦.

- Coffie, W., & Bedi, I. (٢٠١٩). The effects of IFRS adoption and firm size on audit fees in financial institutions in Ghana. ***Accounting Research Journal,*** *32*(٣), ٤٣٦-٤٥٣.

- Corradini, I. (٢٠٢٠). ***Building a Cybersecurity Culture in Organizations***. Springer.

- Donalds, C., & Bryson, K. (٢٠١٩). Toward a cybercrime classification ontology: A knowledge-based approach. ***Computers in Human Behavior***, ٩٢, ٤٠٣-٤١٨.

- Drew, J. (٢٠٢٠). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. ***JOURNAL OF CRIMINOLOGICAL RESEARCH, POLICY AND PRACTICE,*** ٦(١), ١٧-٣٣.

- Furnell, S. (٢٠٢٠). Technology Use, Abuse, and Public Perceptions of Cybercrime. ***The Palgrave Handbook of International Cybercrime and Cyberdeviance.*** Springer.

- Gordon, S. & Ford, R. (٢٠٠٦). On the Definition and Classification of Cybercrime.

- Gordon, L.A., Loeb, M.P. and Zhou, L. (٢٠١١). The impact of information security breaches: has there been a downward shift in costs? ***Journal of Computer Security***, *19*(١), ٣٣-٥٦.

- Haapamäki, E., & Sihvonen, J. (٢٠١٩), Cybersecurity in accounting research, ***Managerial Auditing Journal***, *34*(٧), ٨٠٨-٨٣٤.

- Hamm, K. (٢٠١٩, September ١٩). Cybersecurity: A Holistic Approach. Public Company Accounting Oversight Board (PCAOB). https://pcaobus.org/news-events/speeches/speech-detail/cybersecurity-a-holistic-approach_٧٠٧

- Hay, C.; Knechel, R. and Wong, N. (٢٠٠٦). Audit fees: A meta-analysis of the effect of supply and demand attributes. ***Contemporary Accounting Research,*** *23*(١), ١٥٧-١٩١.

- Januarti, I., & Wiryaningrum, M.S. (٢٠١٨). The effect of size, profitability, risk, complexity, and independent audit committee on audit fee. ***Journal Dinamika Akuntansi,*** *10*(٢), ١٣٦-١٤٥.

- Kanakriyah, Reda. (٢٠٢٠).Model Determine main factors used to measure audit fees. ***Academy of accounting and financial studies journal***, *24*(٢), ١-١٣.

- Kenny, D.A. & Baron, R.M. (١٩٨٦). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. ***Journal of Personality and Social Psychology,*** ٥١(١), ١١٧٣-١١٨٢.

- Kraub, P., Pronobis, P. & Zülch, H. (٢٠١٥). Abnormal audit fees and audit quality: initial evidence from the German audit market. ***Journal of Business Economics volume,*** ٨٥, ٤٥–٨٤.

- Li, H., No, W., & Bortiz, J. (٢٠٢٠). Are External Auditors Concerned about Cyber Incidents? Evidence from Audit Fees. ***AUDITING: A Journal of Practice & Theory,*** ٣٩ (١), ١٥١–١٧١.

- Mphatheni, M., & Malulek, W. (٢٠٢٢). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. ***INTERNATIONAL JOURNAL OF RESEARCH IN BUSINESS AND SOCIAL SCIENCE,*** ١١(٤), ٣٨٤-٣٩٦.

- Ngo,T., & Andrea, T.(٢٠٢١). CYBER-SECURITY RISKS ASSESSMENT BY EXTERNAL AUDITORS. ***Interdisciplinary Description of Complex Systems***.١٩ (٣), ٣٧٥-٣٩٠.

- Otuya. W. (٢٠١٩). Kenny and Baron ٤ Step Analysis (١٩٨٦): A Case of Employee Job Satisfaction as a Mediator between Ethical Climate and Performance among Sugarcane Transport Smes in Western Kenya. ***Journal of Economics and Sustainable Development***, ١٠(١٤).

- Public Company Accounting Oversight Board – PCAOB (٢٠١٠). Identifying and Assessing Risks of Material Misstatement. AS No. ١٢: Public Company Accounting Oversight Board (PCAOB).

- Public Company Accounting Oversight Board – PCAOB (٢٠١٣). Considerations for Audits of Internal Control over Financial Reporting: Public Company Accounting Oversight Board (PCAOB).

- Puchkov, D. (٢٠٢٢). Main Trends in the Development of International Crime in the Implementation of Cyber technologies**.** ***Cybercrimes and Financial Crimes in the Global Era*****.** Springer, ٢٧-٣٤.

- Radoniewicz, F. (٢٠٢٢). ***Cyberspace, Cybercrime, Cyberterrorism. Cybersecurity in Poland***. Springer, ٣٣-٥١.

- Richardson, V., Smith, R., Watson, M. (٢٠١٩). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. ***Journal of Information Systems,*** *33(3), 227-265.*

- Rosita, P., Googling, F., & Lynn, T. (٢٠١٩). Audit Firm Assessments of Cyber- Security Risk: Evidence from Audit Fees and SEC Comment Letters. ***The International Journal of Accounting,*** ٥٤(٠٣).

- Rosati, P., Gogolin, F., & Lynn, T. (٢٠٢٢). Cyber-Security Incidents and Audit Quality. ***European Accounting Review***, ٣١(٣), ٧٠١-٧٢٨.

- Saleh, M., & Magdi, Y. (٢٠٢٣). Determining audit fees: evidence from the Egyptian stock market. ***International Journal of Accounting & Information Management,*** ٣١(٢), ٣٥٥-٣٧٥

- Smith, T., Jones, A., Johnson, L., & Smith, L. (٢٠١٩). Examination of cybercrime and its effects on corporate stock value. ***Journal of Information, Communication and Ethics in Society,*** ١٧(١), ٤٢-٦٠.

- Suryani, D., & Sitorus, T. (٢٠١٨). The client risk and the audit planning: Influence of acceptance of audit engagement. ***International Research Journal of Business Studies,*** *10*(٣), ١٨٣-١٩٨.

- Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., & Kozych, I. (٢٠٢١). Combating cybercrime: economic and legal aspects. ***Wseas Transactions on Business and Econonmics***, ١٨, ٧٥١-٧٦٢

- Thomas, D.; Loader, B. Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age; Thomas, D., Loader, B., Eds.; Routledge: London, UK, ٢٠٠٠

- World Economic Forum. (٢٠١٧). the Global Risks Report ٢٠١٧: ١٢th Edition. Available at: https://www٣.weforum.org/docs/GRR١٧_Report_web.pdf.

- Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (٢٠١٨). The impact of audit firms' Characteristics on audit fees following information security breaches. ***Journal of Accounting and Public Policy***, ٣٧(٦), ٤٨٩–٥.

ثالثاً المواقع الإلكترونية:

- https://egx.com.eg

- www.Mubasher.info