العدد الاول– يناير 2023– المجلد السابع

مجلة الإسكندرية للبحوث المحاسبية
قسم المحاسبة والمراجعة

أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين– دراسة تجريبية

د/ إبراهيم أحمد إبراهيم شرف
أستاذ مساعد بقسم المحاسبة
كلية التجارة – جامعة دمنهور

ملخص البحث

استهدف البحث دراسة واختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. وأيضاً اختبار أثر بعض السمات النوعية للمستثمر (الجنس، والعمر، ومستوي التأهيل العلمي) كمتغيرات معدلة للعلاقة محل الدراسة. ولتحقيق هدف البحث، تم إجراء دراسة تجريبية علي عينة من 108 من أعضاء هيئة التدريس وطلبة الدراسات العليا بكليات التجارة بالجامعات المصرية، كممثلين للمستثمرين غير المحترفين. وقد خلص البحث في شقه التجريبي إلي وجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. كما خلص البحث إلي وجود تأثير معنوي لكل من؛ (الجنس، والعمر، ومستوي التأهيل العلمي للمستثمر) علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين.

الكلمات المفتاحية: إدارة مخاطر الأمن السيبراني– الإفصاح عن إدارة مخاطر الأمن السيبراني– المستثمرين غير المحترفين –جنس المستثمر– عمر المستثمر– التأهيل العلمي للمستثمر.

E.mail: Ibrahim_shraf2000@yahoo.com

The Effect of the companies' disclosure of Cybersecurity Risk Management Report on Non-Professional Egyptian Investors'Decisions - An Experimental Study

Abstract

This research amis to study and investigate The Impact of the companies' disclosure of Cybersecurity Risk Management Report on Non-Professional Egyptian Investors' Decisions. The research also examined the impact of some qualitative characteristics (Gender, age, and investor qualification) on this relation. to achieve the aim of the research an experimental study was conducted on a sample of 108 of Faculty members and postgraduate students in the Faculties of Commerce, in Egyptian Universities as representative of Non-Professional Egyptian Investors. The Experimental Study shows that there is a significant impact of the companies' disclosure of Cybersecurity Risk Management Report on Non-Professional Egyptian Investors' Decisions. The research also concluded that there is a significant effect for each of; (gender, age, and level of educational) on this relation.

Keywords: Cybersecurity Risk Management- Cybersecurity Disclosures- Nonprofessional Investors- Investor Gender- Investor age - Investor qualification.

1- مقدمه البحث

تمثل المعلومات المورد الطبيعي لعالم الأعمال، في كل الدول. ويعتبر نظام معلومات المحاسبية المالية، وما ينتجه من معلومات مصدراً لتلبية احتياجات أصحاب المصالح، وخاصة المستثمرين من هذه المعلومات. لتساعدهم في إتخاذ القرارات الرشيدة. كما يؤثر نظام معلومات المحاسبية المالية ويتأثر بمتغيرات بيئة الممارسة المحاسبية، ومن أهمها تهديدات المخاطر التي تواجهها الشركات (Gao et al., 2020).

ولقد أدى قيام الشركات بتسخير قوة التقدم الكبيرة في تكنولوجيا المعلومات لخدمة أعمالها وتحسين كفاءة عملياتها، إلى تغير بيئة الأعمال بوتيرة سريعة، لمواكبة هذا التقدم، من خلال تبني التقنيات الرقمية الجديدة، وهو ما يظهر في المعاملات والتواصل بين الشركات، وأصحاب المصالح، وما يتضح تأثيره العميق على كل القطاعات الإقتصادية، باعتبارها الثورة الصناعية الرابعة (G.4) الجديدة (Haapamäki & Sihvonen, 2019; Cheong et al., 2021; Walton et al., 2021; Ali et al., 2021).

وعلي الرغم من أن لاستغلال التقدم في تكنولوجيا المعلومات مزايا رائعة، إلا أنها يرافقها عالم متغير من المخاطر والتهديدات والهجمات السيبرانية[1] غير المسبوقة، والتي يتم اعتبارها أكثر المخاطر إثارة للقلق لكل شركة في العالم، والأكثر سوءاً واحتمالا بعد الكوارث الطبيعية (SEC, 2018; Gao et al., 2020; Ali et al., 2021; Barry et al., 2022). ويُنظر إلى تهديدات الأمن السيبراني كأهم التحديات التي تواجهها الشركات، وتمثل تهديدًا حقيقيًا وخطيرًا، تؤثر سلباً علي نموها المستقبلي، لأسباب متنوعة أهمها فقدان الملكية الفكرية، وتعطيل العمليات، وسرقة الأسرار التجارية، وإضطرابات الأعمال ، والإضرار بالسمعة، وفقدان ثقة أصحاب المصالح، والتدهور الذي يحدث في أداء الأسهم وقيمة الاستثمارات، وتكلفة التقاضي[2] (AICPA 2017; Roskot et al., 2020; Nordlund, 2021).

---

(1) استخدمت الدراسات عبارات "مخاطر الإنترنت" ، و"الهجوم السيبراني" ، و"مخاطر وحوادث الأمن السيبراني" ، و"المخاطر الإلكترونية"، "وهجوم الأمن السيبراني"، "وانتهاك البيانات"، "وانتهاك المعلومات"،" واختراق الشبكة".وغيرها وسوف يستخدم الباحث أيان من هذه الالفاظ كمترادفات لنفس المعني(Walton et al., 2021; Chen et al., 2022).

(2) تسببت الحوادث البارزة للأمن السيبراني ، مثل ما تعرضت له شركات Equifax و Sony و Target، لخسائر بعد سلسلة من الانتهاكات السيبرانية، حيث واجهت بالعديد من الدعاوى القضائية الجماعية من جانب أصحاب المصالح Janvrin ;2018 ,.Li et al) (Wang, 2019; Walton et al., 2021; Cheng et al., 2022 &. وزادت تكاليف التعويضات في الولايات المتحدة الأمريكية، من 25 مليون دولار في عام 2014 إلى أكثر من 8 مليارات دولار في عام 2018. كما تشير التقديرات إلى أن الحوادث السيبرانية كلفت الاقتصاد العالمي أقل بقليل من تريليون دولار أمريكي في عام 2020 (Jin, 2015;Calderon & Gao,2021;Cremer et al.,2022).

وقد لاقت مخاطر الأمن السيبراني إهتمامًا متزايدًا منذ السنوات العشر الماضية، من قبل كل من وسائل الإعلام، والشركات، وأصحاب المصالح، والحكومات، وأثارت نقاشًا حادًا بين الهيئات التنظيمية والمهنية، والأكاديميين، والممارسين، وصانعي السياسات، إزاء الجرائم والتهديدات الإلكترونية المتزايدة (Hilary et al., 2016; Li et al., 2018; Janvrin & Wang, 2019; Cheong et al., 2021; Cheng et al., 2022).

وقد أولى المنظمون وواضعوا المعايير إهتمامًا متزايدًا لتعزيز الإفصاح عن مخاطر الأمن السيبراني للشركات(SEC, 2011, 2018; AICPA 2017; Cheng et al., 2022). حيث قدمت SEC إرشادات لتوفير مزيد من الشفافية، وأوصت الشركات بالإفصاح عن إدارة مخاطر الأمن السيبراني ERM، والحوادث السابقة، وأي تكاليف تقاضي ومعالجة مرتبطة بها إن وجدت، واحتمال وحجم أحداث الأمن السيبراني المستقبلية. كما طور المعهد الأمريكي للمحاسبين القانونيين AICPA في عام 2017 إطار عمل لإعداد تقارير إدارة مخاطر الأمن السيبراني لتوجيه الشركات نحو تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني بشكل أفضل، يهدف إلى إفادة مجموعة واسعة من المستخدمين المحتملين بما في ذلك المستثمرين والمحللين الماليين (Berkman et al., 2018; Walton et al., 2021; Nordlund, 2021; Cheng et al., 2022).

وأصبحت الشركات تتعرض لضغوط لإثبات يقظتها وتأكيدها لإدارة تهديدات الأمن السيبراني، من خلال تبنيها لممارسات وسياسات وعمليات وإجراءات رقابية وضوابط مصممة لحماية سرية وسلامة وتوافر معلوماتها وأنظمتها الإلكترونية، للاستجابة، والتخفيف، والتعافي من الانتهاكات والأحداث الأمنية والتهديدات السيبرانية، والتي يمكن أن تعوق تحقيق أهدافها. وبذلك حظي الإفصاح عن إدارة مخاطر الأمن السيبراني باهتمام كبير من جانب أصحاب المصالح كاستجابة لطلبهم للحصول على مزيد من المعلومات، ومن المتفق عليه أن هذه الإفصاحات لها محتوي معلوماتي ينعكس علي قرارات أصحاب المصالح، وبصفة خاصة المستثمرين (Jin, 2015; Li et al., 2018; Janvrin & Wang, 2019; Eaton et al., 2019; Swift et al., 2020; Cheong et al., 2021; Cheng et al., 2022).

وفي الوقت الذي يحتاج فيه المستثمرون إلى معرفة كيفية إدارة الشركة للمخاطر التي تواجهها والاستراتيجيات التي تستخدمها في التعامل معها(Mousa, & Elamir, 2013). إلا أنه من غير الواضح معرفة كيف سيتأثر المستثمرين غير المحترفين(الأفراد) بالإفصاحات عن إدارة مخاطر الأمن السيبراني(AICPA, 2017; Cheng et al., 2022).

وفيما يتعلق بالاهتمام بإدارة مخاطر الأمن السيبراني، في مصر، فهناك إهتمام بالأمن السيبراني علي المستوي الرسمي، فقد احتوي الدستور المصري عام 2014 علي ما يلزم الدولة باتخاذ التدابير للحفاظ علي أمن الفضاء السيبراني، كما تم إنشاء الاستراتيجية الوطنية للأمن السيبراني 2017-2021 لمواجهة المخاطر السيبرانية.

وفيما يتعلق بالدراسات الأكاديمية التي تناولت الإفصاح عن مخاطر الأمن السيبراني في مصر. فمنها دراسة الرشيدي والسيد(2019) والتي اتجهت لاختبار أثر الافصاح عن مخاطر الأمن السيبراني علي أسعار الاسهم وأحجام التداول. كما ذهبت دراسة علي وصالح (2021) لتحليل واختبار أثر الافصاح عن إدارة مخاطر الأمن السيبراني علي قرار الاستثمار بالأسهم. بينما سعت دراسة بدوي (2021) لاختبار أثر جودة ومستوي التوكيد Assurance علي برنامج إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين. **ويسعي البحث الحالي لدراسة أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، نظرياً وتجريبياً**.

2- مشكلة البحث

أصبحت الجرائم السيبرانية تمثل تهديدًا حقيقيًا وخطيرًا للشركات، بسبب فقدان ثقة أصحاب المصالح، والتدهور الذي يؤثر علي أداء الأسهم وقيمة الاستثمارات(Roskot et al.,2020). وقد أثارت المخاوف التي أعرب عنها المنظمون وواضعو المعايير بشأن تهديدات ومخاطر الأمن السيبراني، والتي تؤدي إلى عواقب مالية وسلبية كبيرة على الشركات وعملياتها وتزيد من مخاوف المستثمرين، وقد حظيت مخاطر الأمن السيبراني باهتمام مجتمع الأعمال وأظهر الحاجة إلى مزيد من الإفصاح، باعتبارها أحد العوامل الرئيسية التي قد تؤثر علي قرارات أصحاب المصالح وخاصة المستثمرين (Farkas & Murthy, 2014; Spanos & Angelis, 2016; Perols, 2019; Gao et al., 2020; Kelton, 2021; Ramírez et al., 2022).

وقد اتجهت العديد من الدراسات (Chai & Rao, 2011; Hilary et al., 2016; Morse et al., 2017; Perols, 2019; Frank et al., 2019; Cheng & Walton, 2019; Yang et al., 2020; Kelton & Pennington, 2020; Ali et al., 2021; Cheng et al., 2022) للوقوف علي رد فعل المستثمرين تجاه القضايا المختلفة المتعلقة بالأمن السيبراني، ومنها اختبار تأثير الإفصاح الاختياري عن تقرير إدارة مخاطر الأمن السيبراني علي تصورات ورغبة وأحكام وقرارات المستثمرين، باعتباره أمراً هاماً، يمكن أن يساعدهم على تقييم إمكانية حدوث أحداث سلبية وانتهاك أمن المعلومات في الشركات في المستقبل.

ويُمكن التعبير عن مشكلة البحث في كيفية الإجابة عن الأسئلة التالية نظرياً وتجريبياً في مصر؛ هل يؤثر محتوي إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني في سياق التقارير المالية معنوياً علي قرارات المستثمرين المصريين غير المحترفين بالاستثمار في أسهم هذه الشركات؟. وهل يختلف التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار المستثمرين المصريين غير المحترفين ببعض السمات النوعية والفنية لهم وتحديداً النوع والعمر ومستوي التأهيل العلمي؟.

3-هدف البحث

يستهدف البحث دراسة واختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، وذلك من خلال مدخل نظري تجريبي مبرر وموثق علمياً في البيئة المصرية.

4- أهمية ودوافع البحث

تتمثل أهمية هذا البحث **أكاديمياً** من خلال تناوله لموضوع إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وتقييم أثره علي قرارات المستثمرين غير المحترفين. فعلى الرغم من الأهمية الكبيرة للأمن السيبراني وتأثيرها الجوهري على العمليات التجارية ونزاهة التقارير المالية للشركات، إلا أن هناك ندرة في البحوث التجريبية بشأن تأثير ممارسات الإفصاح عن مخاطر الأمن السيبراني على قرارات أصحاب المصالح وأحكام المستثمرين غير المحترفين. **كما يسعي البحث** لدراسة واختبار تأثير الاختلافات والتشابهات في السمات النوعية والفنية للمستثمرين الأفراد غير المحترفين وتحديداً النوع والعمر ومستوي التأهيل العلمي علي العلاقة محل الدراسة. وبذلك يحاول هذا البحث تضييق الفجوة بين الدراسات الأكاديمية التي تمت في دول متقدمة، والدراسات التي تمت في مصر في هذا المجال. وأما **عملياً** فتتمثل أهمية البحث في أنه يأخذ جانب المبادرة في تقديم مقترح لتقرير إفصاح الشركات عن إدارة مخاطر الأمن السيبراني مشتق من الإصدارات الدراسات السابقة، واختبار أثر الإفصاح عنه علي قرارات المستثمرين غير المحترفين. كخطوة نحو توضيح أهمية الدور الهام والفعال الذي يلعبه الإفصاح عن إدارة الأمن السيبراني، في بيئة الأعمال المصرية من ناحية. ودفع وتوجيه الشركات إلى الاهتمام بإدارة مخاطر الأمن السيبراني لديها والإفصاح عنه، للتخفيف من مخاوف أصحاب المصالح وخاصة المستثمرين حول ما إذا كانوا يديرون مخاطر الأمن السيبراني الخاصة بهم بشكل فعال، ولما لها من فوائد وتأثير علي أداء الشركات.

وكذلك لفت انتباه الجهات التنظيمية وواضعي المعايير وصانعي السياسات بشأن أهمية مخاطر الأمن السيبراني، لما لها من تأثير سلبي محتمل وعواقب اقتصادية علي الشركات، والأحكام الاستثمارية

للمستثمرين وأصحاب المصالح، الأمر الذي يُمكن أن يكون له مردود إيجابي علي قراراتهم، في محاولة لإثراء المردود العملى للبحث المحاسبي في هذا المجال.

ومن أهم دوافع البحث سعيه لمحاولة توفير فهم أكثر تعمقًا لتأثير بعض العوامل على تصورات وعملية صنع القرار لدى المستثمر غير المحترف، بصرف النظر عن العوامل الأخرى. كما ينتهج البحث منهجاً تجريبياً لاختبار العلاقة محل الدراسة متلافياً بذلك عيوب المنهجية الميدانية بقائمة الاستقصاء في كثير من البحوث المصرية السابقة.

5- حدود البحث

يقتصر البحث علي دراسة واختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، وذلك في بيئة الأعمال المصرية، ومدي تأثر هذه العلاقة ببعض السمات النوعية والفنية للمستثمرين مثل؛ جنس المستثمر، وعمره، ومستوي تأهيله العلمي. وبذلك يخرج عن نطاق البحث المستثمرين المحترفين ومديري صناديق الاستثمار بالبنوك وأصحاب المصالح الآخرين، وتوقيت وجودة الإفصاح عن مخاطر الأمن السيبراني. وكذلك يخرج عن نطاق البحث، حتمية تعرض الشركة لحوادث سيبرانية سابقة والاختلافات في أنواعها وجوهريتها وأهميتها النسبية. كما يخرج عن نطاق البحث السمات الشخصية الأخرى للمستثمر غير المحترف مثل؛ القدرة الفطرية، الحالة المزاجية، والجوانب النفسية، والحالة الاجتماعية. كما يخرج عن نطاق البحث نوع الصناعة الذي تنتمي إليها الشركة، وأدائها المالي، وكفاءة الإدارة، وفعالية هيكل الرقابة الداخلية. كما أن قابلية النتائج للتعميم مشروطة بحدود البحث وضوابط اختيار مجتمع وعينة الدراسة وكيفية قياس متغيرات الدراسة.

6- خطة البحث

انطلاقاً من مشكلة البحث والهدف منه وفي إطار حدوده يُستكمل البحث علي النحو التالي:

6-1 الإفصاح عن إدارة مخاطر الأمن السيبراني(المفهوم والمحتوي والمحددات والأهمية والمردود).

6-2 قرار الاستثمار في الأسهم من منظور المحاسبة المالية في بيئة تكنولوجيا المعلومات.

6-3 تحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم وإشتقاق فرض البحث الأول.

6-4 تحليل أثر السمات النوعية والفنية للمستثمرين المصريين غير المحترفين علي العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارهم بالاستثمار في الأسهم وإشتقاق فروض البحث من الثاني حتي الخامس.

6-5 منهجية البحث (التحليل الأساسي والتحليلات الأخري).

6-6 نتائج البحث والتوصيات ومجالات البحث المقترحة.

6-1 الإفصاح عن إدارة مخاطر الأمن السيبراني(المفهوم والمحتوي والمحددات والأهمية والمردود)

فيما يتعلق بمفهوم الأمن السيبراني، فقد أشار Craigen et al. (2014) إلي أن **الأمن السيبراني** Cybersecurity هو جمع وتنظيم الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني، والأنظمة الأخري التي تدعم الفضاء الالكتروني من الأحداث والهجمات والتي تتعارض فعلياً مع القانون والملكية. وعرف AICPA (2017) الأمن السيبراني ، علي أنه مجموعة التقنيات والعمليات والاجراءات المصممة لحماية الشبكات والأنظمة وأجهزة الكمبيوتر والبرامج وقواعد البيانات من الهجوم الالكتروني أو التلف أو الوصول غير المصرح به، أو التعطيل أو الاستغلال غير المشروع. كما عرفت **الهيئة الوطنية للأمن السيبراني(2018) الأمن السيبراني** علي أنه مجموعة من التقنيات والعمليات لحماية أجهزة الكمبيوتر وقواعد البيانات والشبكات والتطبيقات وما تحتوية من بيانات وخدمات من الهجمات الالكترونية، والوصول غير المصرح به، والتغيير أو التعطيل وسوء الاستخدام، أو الاستغلال غير المشروع.

ويوضح Gao et al.(2020) أن الأمن السيبرانى أو الإلكتروني بأنه نشاط أو عملية أو قدرة أو قابلية أو الحالة التي يتم بموجبها حماية أنظمة المعلومات والاتصالات والمعلومات الواردة فيها و/ أو الدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل، أو الاستغلال.

ويري Cheng et al.(2022) أن الأمن السيبراني غالبًا ما يُعتبر جزءًا من أمن تكنولوجيا المعلومات، ويتمثل في الإحتياطات المتخذة للحماية من الجرائم التي الإلكترونية، وخاصة الوصول غير المصرح به إلى أنظمة الكمبيوتر والمعلومات المتصلة بالإنترنت.

وفيما يتعلق بمخاطر الأمن السيبراني Cybersecurity Risks فقد عرفت، الهيئة الوطنية للامن السيبراني (2018) مخاطر الأمن السيبراني علي أنها المخاطر التي تهدد عمليات الشركة بما فيها رؤية الشركة أو رسالتها أو إداراتها أو صورتها أو سمعتها أو أصولها بسبب إمكانية الوصول غير المصرح به أو سوء الاستخدام أو الافصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات. كما عرفها Frank et al.(2019) علي أنها أي حدث يهدد أو يشكل تهديدًا لنظام المعلومات أو المعلومات التي يعالجها النظام أو يخزنها أو ينقلها. كما يري Swift et al.(2020) مخاطر الأمن السيبراني على أنها حدث يهدد سرية وسلامة وتوافر المعلومات، وانتهاكها من جانب طرف غير مصرح له.

أما إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management فد عرفها AICPA (2017) علي أنها عملية تنفيذ الشركة لمجموعة من السياسات والعمليات والاجراءات الرقابية والضوابط

المصممة لحماية معلوماتها وأنظمتها الالكترونية من الأحداث والتهديدات السيبرانية التي يمكن أن تعوق تحقيق أهداف الشركة.

أما الإفصاح عن إدارة مخاطر الأمن السيبراني فيعني قيام إدارة الشركة بتوصيل معلومات بشأن تصميمها وتنفيذها لمجموعة من السياسات والعمليات والإجراءات الرقابية والضوابط لحماية معلوماتها وأنظمتها الالكترونية من الأحداث والتهديدات السيبرانية والتي يمكن أن تعوق تحقيق أهدافها (AICPA 2017; Frank et al.,2019).

ويخلص الباحث مما سبق إلي أن حماية الأنظمة الإلكترونية والفضاء السيبراني وأمن تكنولوجيا المعلومات يتطلب من الشركة، القيام بعمليات لإدارة هذه المخاطر. **ويري الباحث أن إدارة مخاطر الأمن السيبراني** تتعلق بقدرة الشركة علي جمع وتنظيم الموارد وتنفيذ مجموعة من التقنيات والعمليات والهياكل المستخدمة والسياسات والاجراءات الرقابية والضوابط المصممة لدعم الفضاء الالكتروني وتوفير الحماية لأجهزة الكمبيوتر والشبكات وقواعد البيانات والتطبيقات من الهجمات الالكترونية أو التلف أو الوصول غير المصرح به، أو التعطيل أو الاستغلال غير المشروع، والذي يهدد سرية وسلامة وتوافر المعلومات ويعطل الشركة عن تحقيق أهدافها.

وفيما يتعلق بالنظريات المفسرة لإفصاح الشركات عن مخاطر الأمن السيبراني، يري(2008) Iatridis أنه وفقاً لنظرية أصحاب المصالح فإن الشركة يجب أن توفر لأصحاب المصالح أنواعًا مختلفة من المعلومات لتلبية احتياجاتهم المختلفة، ومنها الإفصاح عن المخاطر التي تواجهها الشركة. كما أشار Khalil, & Maghraby (2017) إلي أنه يمكن تفسير ممارسات الإفصاح عن المخاطر، في ضوء نظرية الوكالة، حيث يفصح المديرون عن مزيد من المعلومات لتقليل تكاليف الوكالة ولإقناع المستثمرين بأن عملهم على النحو الأمثل. وإظهار جهودهم في تحقيق هدف تعظيم ثروة المساهمين وتخفيض عدم تماثل المعلومات. بينما يري(2018) Sulistyaningsih & Gunawan أنه وفقا لنظريةً الإشارة توفر الإدارة معلومات حول المخاطر من خلال التقارير المالية، لإظهار مزيد من الشفافية عن الأداء الجيد ، لتحسين سمعة الشركة، ولجذب المستثمرين، وزيادة قيمة الشركة. في حين يوضح (2022) D'Arcy & Basoglu أنه وفقاً للنظرية المؤسسية، توجد ضغوط مؤسسية ومطالبات في الصناعة بتغيير ممارسات الإفصاح الخاصة بها، كما أن الشركات تقلد سلوك أقرانها في الصناعة. وكذلك أوضح أنه وفقاً للنظرية الشرعية فإن الشركات تفصح عن المعلومات لأصحاب المصالح من المستثمرين والمشاركين الآخرين في السوق لمساعدتهم في تقييم الشركة، وبالتالي تحافظ على شرعيتها من خلال الإفصاح عن المعلومات التي تتماشى مع توقعات المستثمرين.

وفيما يتعلق بالإصدارات بشأن إدارة مخاطر الأمن السيبراني؛ فقد وضع المعهد الأمريكي للمحاسبين القانونيين AICP **في عام 2017** إطارا للتقرير عن إدارة مخاطر الأمن السيبراني بهدف دعم الشركات وإرشادها في الإفصاح عن مخاطر الأمن السيبراني. وتتضمن **معايير وصف إدارة برنامج الأمن السيبراني للشركة** description criteria، وذلك لوصف برنامج إدارة مخاطر الأمن السيبراني للشركة. والذي يتمثل في مجموعة من السياسات والعمليات والضوابط المصممة لحماية المعلومات والأنظمة من الأحداث السيبرانية التي يمكن أن تعوق تحقيق أهداف الشركة، والإفصاح والاستجابة والتخفيف والتعافي من الأحداث السيبرانية التي لم يتم منعها في الوقت المناسب. ويقدم إرشادات للتنفيذ لكل معيار. والعوامل التي يجب مراعاتها حول طبيعة ومدى الإفصاحات الذي يتطلبه كل معيار وذلك كما يلي: **فيما يتعلق بمعايير وصف برنامج إدارة مخاطر الأمن السيبراني، تتمثل في؛** طبيعة أعمال الشركة وعملياتها، والأنواع الرئيسية للمعلومات الهامة التي تم إنشاؤها أو جمعها أو إرسالها أو استخدامها أو تخزينها بواسطة الشركة بما فيها المعلومات المتعلقة بالأفراد التي تستدعي الحماية بناءً على القانون أو الالتزام أو توقع معقول للسرية. **وفيما يتعلق بأهداف برنامج إدارة مخاطر الأمن السيبراني** فإنها تتمثل في توافر سرية وتوافر وسلامة المعلومات، ويجب الأخذ في الاعتبار الالتزامات التي تم التعهد بها، والقوانين واللوائح المعمول بها، ومعايير الصناعة، والإتاحة وتمكين الوصول في الوقت المناسب، وأن يتم تحديد أهداف الأمن السيبراني بناءً على أعمال الشركة وأهدافها الإستراتيجية وتطوير والحفاظ على الضوابط داخل الشركة. **والعوامل التي لها تأثير كبير على المخاطر المتلازمة Inherent بالأمن السيبراني، متمثلة في** الخصائص والبيئة التكنولوجية، والتغييرات التنظيمية خلال الفترة التي يغطيها الوصف للشركة وبيئتها. **وفيما يتعلق بهيكل حوكمة إدارة مخاطر الأمن السيبراني، فتشمل التقرير عن النزاهة والأخلاق وإشراف مجلس الادارة على مخاطر الأمن السيبراني. وفيما يتعلق بعملية تقييم مخاطر الأمن السيبراني،** يجب تحديدها في ضوء الاعتبارات البيئية والتكنولوجية، والتغييرات التنظيمية، وتقييم المخاطر ذات الصلة بتحقيق الشركة لأهدافها والتي يمكن أن يكون لها تأثيراً جوهرياً على ادارة مخاطر الأمن السيبراني. وكذلك تحديد وتقييم وإدارة المخاطر المرتبطة بالموردين وشركاء العمل. **وفيما يتعلق بقنوات إتصال الأمن السيبراني وجودة معلومات الأمن السيبراني يجب الأخذ في الاعتبار** عملية الاتصال الداخلي بمعلومات الأمن السيبراني الضرورية ودعم أداء برنامج إدارة مخاطر الأمن السيبراني. **وفيما يتعلق بعملية رقابة برنامج إدارة مخاطر الأمن السيبراني يجب الأخذ في الاعتبار** إجراء تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني. **وفيما يتعلق بعمليات رقابة الأمن السيبراني، يجب الأخذ في الاعتبار** مواءمة الضوابط مع الاستجابة للمخاطر. **والبنية التحتية لتكنولوجيا المعلومات للشركة، وفيما يتعلق بسياسات الأمان الرئيسية والعمليات يجب الأخذ في الاعتبار** ضرورة وجود سياسة أمنية رسمية لتنفيذ الأمن السيبراني للشركة لتمنع الأحداث السيبرانية المتعمدة وغير المتعمدة. **وفيما يتعلق**

بالاستجابة للحوادث السيبرانية المحددة والتعافي منها؛ لابد من التقرير عن الأحداث السيبرانية المحددة إلى الأطراف المناسبة، وتقييم الحوادث السيبرانية، والإجراءات اللازمة للاستجابة وتقييم وتخفيف الضرر (AICP, 2017).

وبشأن لجنة تداول الأوراق المالية بالبورصة الأمريكية SEC فقد قامت في13 أكتوبر 2011 بنشر توجيهات للشركات المسجلة بالبورصة بشأن الإفصاح عن مخاطر الأمن السيبراني، وما يجب أن تتخذه الشركات في الإعتبار عند تقييم المخاطر السيرانية، تساعد في تقييم ما يجب تقديمه من إفصاحات حول مسائل الأمن السيبراني، في ضوء الحقائق والظروف الخاصة بكل شركة. متناولة مناقشة متطلبات الإفصاح حول مخاطر الأمن السيبراني، وعوامل الخطر والحوادث السيبرانية السابقة وشدة وتواتر تلك الحوادث.

وفي 20 فبراير 2018 أصدرت SEC دليلاً إرشادياً وتفسيرياً بشأن الإفصاح عن مخاطر الأمن السيبراني، ويتضمن قسمين؛ ويتناول **القسم الأول** طبيعة الأمن السيبراني وتعريفه ومخاطره وأثاره السلبية علي المستثمرين، وأهمية الإفصاح للأطراف المعنية، وأثارها علي الشركة وعملياتها. وإرشادات الإفصاح عن مخاطر الأمن السيبراني وأهمية اتجاه الشركات للإفصاح، والتوسع في متطلبات الإفصاح عن تلك الصادرة في 2011 متناولة حوادث الأمن السيبراني وتقديم معلومات عن الأحداث الجوهرية، وعلاقة الأطراف ذوي العلاقة بالتعاملات في حالة حدوث حوادث سيبرانية. كما يتناول **القسم الثاني؛** مراجعة القواعد بشأن الافصاح عن مشكلات الأمن السيبراني، متناولاً أهمية مراعاة كل من الأهمية النسبية وعوامل الخطر والموقف المالي ونتائج العمليات وطبيعة النشاط، والسياسات وإجراءات الرقابة، والإفصاح عن تعامل الشركة مع المخاطر السيبرانية.

وفي 9 مارس 2022، أصدرت SEC تعديلات على قواعدها بشأن متطلبات الإفصاح المتعلقة بإدارة مخاطر الأمن السيبراني، متضمنة الإفصاح عن حوادث الأمن السيبراني غير الفردية غير الجوهرية والتي تصبح جوهرية في المجمل، وإعداد تقارير سنوية حول خبرة مجلس الإدارة في مجال الأمن السيبراني ان وجدت، والتأكد من أن سياسات الاستجابة للحوادث السيبرانية توفر مسارًا واضحًا، وإجراء تقييم للأهمية النسبية للحوادث السيبرانية في أقرب وقت قدر المستطاع بعد معرفة الحادث، والإفصاح بشكل دوري عن الاستراتيجية والسياسات والإجراءات المتبعة في حوكمة مخاطر الأمن السيبراني، و تحديد المسؤول عن حوكمة الأمن السيبرانية.

كما قامت لجنة COSO في عام 2015 بوضع وتصميم إطار لإدارة المخاطر السيبرانية طبقاً لإطارها لعام 2013، لدعم الشركات في كيفية الاستخدام والاعتماد على التكنولوجيا المتطورة، ولكن دون توفير

محتوي مرتبط بالمفاهيم الاساسية لإدارة المخاطر السيبرانية، ولا دليلاً تنفيذا. **وفي عام 2017 قامت لجنة COSO**، بتحديث إطار إدارة المخاطر المؤسسية (Enterprise Risk Management (ERM، وكانت الدوافع وراء ذلك، هو ضرورة قيام الشركات بتحسين مدخل إدارة المخاطر السيبرانية لتلبية متطلبات بيئة الأعمال المتطورة. من منطلق أن المخاطر السيبرانية لا يمكن تجنبها ولكن يجب إدارتها، وتشمل الإفصاح المناسب عن عوامل الخطر السيبراني، وإشراف مجلس الإدارة علي إنشاء فريق إدارة المخاطر السيبرانية متعدد الوظائف، والاستثمار في التدريب السيبراني المستمر لتعزيز وعي العاملين بها والمسائلة، ودمج إدارة المخاطر السيبرانية في الخطة الإستراتيجية للشركة، وتحديد وتقييم المخاطر السيبرانية وفقا لطبيعة الصناعة التي تنتمي لها والقضايا البيئية، وإحتمالية وجود دوافع، ووقوع أحداث تؤثر سلبًا على تحقيق أهداف الشركة، والتقييم المستمر والتأكيد على فعالية إدارة الأمن السيبراني والتواصل الداخلي في الأمور المتعلقة بالمخاطر الإلكترونية، للمساعد في منع أو تخفيف تأثير الحوادث السيبرانية، والإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية للأطراف ذات الصلة.

وفي كندا فقد أصدر معهد المحاسبين القانونيين الكندي (2017) CPA– Canada إرشادات للشركات المسجلة بالبورصة بشأن الإفصاح عن مخاطر الأمن السيبراني، والآثار المحتملة للحوادث السيبرانية القوائم المالية للشركات وأدائها المستقبلي، وإمكانية التخفيف من الحوادث السيبرانية، والافصاح عن الإجراءات الحوكمية.

وقد أصدرت هيئة سوق المال السعودية في عام 2019 دليلاً بشأن الأمن السيبراني لمساعدة الشركات في تبني أفضل الممارسات الدولية بشأن إدارة مخاطر الأمن السيبراني. وإصدار إطار تنظيمي للأمن السيبراني في قطاع تكنولوجيا المعلومات في عام 2020.

وبشأن الإهتمام بمخاطر الأمن السيراني في مصر، فقد تناول الدستور المصري عام 2014 في المادة (31) ما يلزم الدولة باتخاذ التدابير للحفاظ علي أمن الفضاء السيبراني وفقاً للقانون، كما تم إنشاء الاستراتيجية الوطنية للأمن السيبراني 2017–2021 مواجهة المخاطر السيبرانية، بهدف حماية وتأمين البنية التحتية للاتصالات والمعلومات وتحقيق بيئة رقمية أمنة في شتي المجالات. وتشمل التحديات والأخطار السيبرانية، وأهم القطاعات الحيوية المستهدفة، وعناصر خطورة التهديات السيبرانية.

ومن خلال استعراض الإصدارات السابقة يتضح أن الأمن السيبراني ليس مجرد مشكلة تتعلق بتكنولوجيا المعلومات؛ ولكن يمثل إحدى مشكلات إدارة مخاطر الشركة التي تتطلب حلاً شاملاً. وتمثل مخاطر الأمن السيبراني مصدر قلق تنظيمي شديد، وتسعي السلطات التنظيمية لمعالجته.

وبشأن توصيف هذا الإفصاح يري الباحث أنه ليس معياريًا، بل إنه إفصاح مرن غير مالي بطبيعته ويكون إجبارياً إذا تضمنت أطر إعداد التقرير المالي وجوب تفعيله كما أنه يمكن أن يكون سنوياً أو حتي فورياً ويمكن أن يكون ورقياً أو رقمياً(RR). كما أن الجهود في مجال الأمن السيبراني غير كافية لمعالجة المخاطر التي قد تواجهها الشركات. حيث تستجيب بعض الشركات بالإفصاح ، بينما يظل البعض الآخر لا يفصح. كما أن إدارات الشركات، لديها الكثير من السلطة التقديرية في تقرير ما إذا كان أو ماذا أو مقدار المعلومات التي تفصح عنها. كما يترك للشركات لتقرر ما إذا كان انتهاك الأمن السيبراني جوهريًا أم لا، وإذا لم يكن الأمر جوهريًا، فسيكون للشركات الحرية في إتخاذ قرار بشأن مقدار المعلومات عن الانتهاكات التي ترغب في الإفصاح في قوائمها المالية. **كما يري الباحث** أن الإصدارات السابقة تعد خطوة أولى حاسمة نحو تمكين الشركات للتواصل بنجاح مع أصحاب المصالح الرئيسيين حول كيفية إدارة مخاطر الأمن السيبراني. كما يجب أن تكون عمليات الإفصاح عن مخاطر الأمن السيبراني متسقة مع الإفصاح عن المخاطر التشغيلية والمالية الأخرى. كما يجب إعادة تقييم إرشادات الإفصاح عن الأمن السيبراني، وجعلها قاعدة تشريعية ملزمة، للشركات بما يؤدي إلى تحسين الشفافية، وعملية اتخاذ القرارات من جانب المستثمرين.

وفيما يتعلق بمحتوي إفصاح الشركات عن مخاطر الأمن السيبراني، أمكن اشتقاق نموذج مقترح للتقرير عن إدارة مخاطر الأمن السيبراني التي تواجهها الشركات، من إجراء خلال إجراء مسح لمجموعة من الإصدارات المحاسبية والمهنية والدراسات، حيث تم الاتفاق علي مجموعة من البنود وفقاً لكل من (SEC, 2011, 2018, 2022; Coso, 2015; Galligan & Rau, 2015; AICPA, 2017; CPA–Canada, 2017; CSA, 2017; Coso, 2020; Galligan et; al., 2020 الدليل التنظيمي للامن السيبراني، 2020; الاستراتيجية الوطنية للأمن السيبراني،2017، وتقوم الشركة بالإفصاح والتقرير عن البنود التالية ضمن مرفقات القوائم المالية[1]، **وذلك كما يلي:**

- إنشاء إدارة خاصة للأمن السيبراني، وإنشاء فريق إدارة المخاطر الإلكترونية متعدد الوظائف، ويقوم مجلس الإدارة بالاشراف عليها، وتدمج الشركة إدارة المخاطر السيبرانية في الخطة الإستراتيجية للشركة.
- تحديد واضح لأهدافها المتعلقة بعملياتها وتقاريرها المالية وغير المالية، لتتمكن من إدارة المخاطر السيبرانية التي تواجهها، والتي تؤثر على تحقيقها لأهدافها، وإتخاذ القرارات بشأن الرقابة عليها.

[1] عرف معيار المراجعة الدولي ISA 720 مرفقات القوائم المالية التي روجعت علي أنها المعلومات الأخرى المالية وغير المالية التي يتم إدراجها، إما عن طريق القانون أو اللوائح أو العرف، في كتيب سنوى يتضمن القوائم المالية محل المراجعة وتقرير مراجع الحسابات بشأنها.

- تصميم هيكل رقابة للأمن السيبراني لمواجهة المخاطر وتقوم بعمل تقييم مستمر للتأكد من فاعلية تصميم وتشغيل الضوابط الداخلية، ومعالجة أوجه القصور واتخاذ الإجراءات التصحيحية.
- الأنشطة والسياسات والاجراءات الرسمية للرقابة العامة على التكنولوجيا لضمان المخاطر السيبرانية عند مستوى مقبول.
- تحديد وتحليل وتقييم المخاطر السيبرانية التي تواجهها، والنظر في احتمالية وقوعها من حيث حجم وكم ونوع تلك المخاطر، والتكاليف والعواقب المحتملة الناتجة عن تلك الحوادث، والتي تؤثر على تحقيق أهدافها؟.
- تقييم المخاطر بطريقة شاملة، متضمنة مدى كفاية الإجراءات الوقائية المتخذة لتقليل مخاطر الأمن السيبراني وتأخذ في الاعتبار مخاطر الصناعة، والاعتبارات البيئية والتكنولوجية، والتغييرات التنظيمية والتغييرات الأخرى.
- نشر أنشطة الرقابة، في شكل مجموعة من السياسات، والإجراءات والضوابط التي تمنع أو تكتشف الانتهاكات السيبرانية، في حالة حدوثها، وتقوم بالافصاح عنه، واتخاذ الإجراءات التصحيحية، وتطوير أنشطة الرقابة التي تساهم في التخفيف من المخاطر إلى مستويات مقبولة.
- دعم هيكل الرقابة الداخلية بالمزيد من المعلومات الخارجية ذات الصلة التجارية والصناعية، ومشاركة هذه المعلومات بين شركاء الأعمال والتحالفات الموثوقة، والتي يمكن أن تساعد في منع أو اكتشاف المخاطر السيبرانية.
- إنشاء قنوات للتواصل وتبادل المعلومات داخل الشركة بين جميع العاملين في كل المستويات، فيما يتعلق بأهداف ومسؤوليات الرقابة الداخلية، لمساعدة الإدارة، والأفراد الذين يضطلعون بمسؤولياتهم المتعلقة بالرقابة الالكترونية.
- التواصل مع الأطراف الخارجية من العملاء وشركاء الأعمال، والمنظمين، والمحللين الماليين، والجهات الحكومية، وأطراف خارجية أخرى بخصوص المخاطر السيبرانية، والتي تؤثر على تيسير عمل الرقابة الداخلية، وتسبب ضرر محتمل.
- الاستعانة بمتخصصين مؤهلين في مجال المخاطر الإلكترونية.
- إجراء تقييم مستمر للتغييرات التي تطرأ والمتعلقة، بالأفراد، والعمليات، والتقنيات، والتي يمكن أن تؤثر على فاعلية هيكل الرقابة الداخلية، وعمل تحديث لتقييم المخاطر على أساس مستمر لتعكس التغييرات.

- إجراء تقييم مستمر ودوري للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني، والضوابط للتأكيد على فعالية إدارة الأمن السيبراني، بهدف تقليل التعرض المحتمل للمخاطر السيبرانية.
- الإلتزام بالإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية وخاصة الحوادث الجوهرية وغير الجوهرية والتي تكون في المجمل جوهرية، في حالة حدوثها خلال السنة السابقة ، وأنواعها ومدي تكرارها.
- إجراء تقييم للأهمية النسبية للحوادث السيبرانية في أقرب وقت قدر المستطاع بعد معرفة الحادث.
- وصف للتغطية التأمينية ذات الصلة بالحوادث السيبرانية، والتكاليف والعواقب الأخرى.
- التدريب المستمر للعاملين لتعزيز وعيهم بشأن الانتهاكات السيبرانية.
- الإفصاح الدوري عن الاستراتيجيات والسياسات والإجراءات المتبعة في حوكمة مخاطر الأمن السيبراني، وتحدد المسؤول عن حوكمة الأمن السيبراني.
- الالتزام بالتقرير عن النزاهة والأخلاق وفقا لمعايير السلوك بالشركة ، وتحديد ومعالجة الانحرافات، لدعم أداء برنامج إدارة مخاطر الأمن السيبراني.

وفيما يتعلق بمحددات الإفصاح عن إدارة مخاطر الأمن السيبراني، يري (Gordon et al., 2010; Kwon et al., 2013) أنها ترجع الضغط المحيط بعملية خرق أنظمة المعلومات ومدي تأثيره على تقييم أصحاب المصالح لقيمة للشركة. بينما يوضح Amir et al. (2018) أن الشركات لا تقوم بالتقرير عن المعلومات المتعلقة بالهجمات الأكثر خطورة، إلا عندما يكون هناك احتمال لإكتشاف المستثمرين بالفعل لتلك الهجمات. كما يوضح Abdullah (2019) أن حجم الشركة، وربحيتها، وطبيعة الصناعة التي تنتمي إليها، ومدي التأثير علي قيمة الشركة لها تأثير كبير في إفصاح الشركات عن المخاطر.

كما يري Gao et al. (2020) أن الزيادة في الإفصاح عن الأمن السيبراني مدفوعة بشكل أساسي ببعض العوامل منها؛ طبيعة الصناعات مثل خدمات المستهلك، والبرمجيات والخدمات، والخدمات المصرفية، وكذلك إرشادات SEC، ومخاطر الأمن السيبراني العامة، والعدد الإجمالي للحوادث الأمنية، وحجم الشركة، وحوادث الأمن السيبراني السابقة. بينما يري Nordlund (2021) أن هناك ثلاثة دوافع تشجع الشركات للإفصاح عن إدارة مخاطر الأمن السيبراني وهي خدمة المستثمر، وخوف إدارة الشركة من تشويه السمعة وتعرضها للعقوبات بسبب انتهاك البيانات، وفي حالة كون انتهاك المعلومات غير جوهري.

ولخص D'Arcy & Basoglu (2022) ما جاء سابقاً بأن ممارسات الشركات تجاه الإفصاح الاختياري عن مخاطر الأمن السيبراني تتمثل في عدة محددات ، منها الضغط الخارجي العام والمؤسسي والذي يؤثر علي سياسة الشركات تجاه قرارات الإفصاح الاختياري، وكذلك طريقة إدارة الشركة لسمعتها والتوافق مع توقعات المستثمرين، وكإستجابة لجهود التخفيف من المخاطر خصوصاً مع حدوث انتهاكات سابقة للأمن السيبراني، والمبادرات التنظيمية مثل إرشادات SEC بشأن تنظيم الإفصاح، والإهتمام الإعلامي، وكذلك رؤية الشركة، وطبيعة الصناعة التي تنتمي اليها وتعرض بعض الشركات في نفس الصناعة لانتهاكات وما يرتبط بها من رد فعل المستثمرين.

ويخلص الباحث مما سبق إلي أن محددات الإفصاح عن مخاطر الأمن السيبراني ترجع للعديد من العوامل، منها الضغوط المؤسسية والإهتمام الإعلامي العام المتعلق بإنتهاك أنظمة المعلومات، وتأثيرها علي قيمة الشركات، والمبادرات والإرشادات التنظيمية، وعدد الحوادث السيبرانية السابقة، وحجم الشركة، وخدمة المستثمر ومقابلة توقعاته، واحتمال تشويه السمعة، والتعرض للعقوبات، وطبيعة الصناعة التي تنتمي إليها، وردود أفعال المستثمرين تجاه أحداث إنتهاك سابقة على مستوى الصناعة.

وفيما يتعلق بأهمية ومردود الإفصاح عن إدارة مخاطر الأمن السيبراني، فقد اتفق البعض (Kahyaoglu & Caliyurt, 2018; Agrafiotis et al., 2018; Kamiya et al., 2018; Islam et al., 2018) علي أن مخاطر الأمن السيبراني تعد أحد أهم التحديات التي تواجه الشركات، فالتعرض للهجمات السيبرانية يسبب معاناة طويلة من الناحية الإقتصادية، وفقدان السمعة. كما أوضح Ramírez et al.(2022) أن الأمن السيبراني أصبح مسؤولية لا مفر منها.

وقد أشار (Abdullah et al., 2015; Abdullah, 2019) إلي أن الإفصاح عن المخاطر يعد إحدى الطرق لزيادة المصداقية وحماية ومساعدة المستثمرين وزيادة ثقتهم في أداء الشركة.

كما أكد Li et al. (2018) علي أهمية الإفصاح عن مخاطر الأمن السيبراني في مساعدة أصحاب المصالح في تقييم إمكانية حدوث أحداث سلبية في المستقبل. وتزويد المنظمين بمعلومات لتشجيع الشركات على الإفصاح عن المزيد عن مخاطر الأمن السيبراني.

في حين يري Frank et al. (2019) أن أهمية التقرير عن الأمن السيبراني تتمثل في تقليل عدم التأكد، وجذب المستثمرين، ويعطي وأصحاب المصالح وشركاء الأعمال معرفة وثقة هائلة في مجهودات الشركة نحو إدارة مخاطر الأمن السيبراني. وفي نفس الاتجاه أشار Cheong et al. (2021) إلي أن الإفصاح عن مخاطر الأمن السيبراني يقلل من تكاليف التقاضي المحتملة التي قد تتعرض لها الشركات، ويزيد

الشفافية، ويبث إشارات إيجابية إلى السوق، بحسن بالتواصل مع أصحاب المصالح ، بشأن الجهود المبذولة لتقليل مخاطر الأمن السيبراني.

ويشير Kelton (2021) إلي أن الإفصاح الاختيارى عن مخاطر الأمن السيبراني يمكن أن يوفر الحماية للشركات من آثار العدوى، من الشركات الأخرى في نفس الصناعة، وكذلك بناء ثقة مع أصحاب المصالح حول كيفية تحديد أولويات الأمن السيبراني وإدارته باعتباره خطرًا مؤسسيًا مهمًا وفرصة استراتيجية مفادها إعلام المستثمرين بإيجابية الشركات تجاه تعزيز مواجهة مخاطر الأمن السيبراني. بينما يري Nordlund(2021) أن إدارات الشركات تفصح عن مخاطر الأمن السيبراني لتحقيق المصالح الذاتية للمديرين من خلال تقليل عواقب مخاطر السمعة المرتبطة بانتهاك للبيانات.

كما أوضح Walton et al.(2021) أنه بشكل عام، يعد الإفصاح عن مخاطر الأمن السيبراني سلاح ذو حدين لأنه يمكن أن يقلل من عدم تماثل المعلومات، ويمكن من التنبؤ بحوادث الأمن السيبراني المستقبلية، ويقلل من تكاليف التقاضي وتدهور السمعة، في حين يمكن أن يزيد أيضًا من احتمال وقوع حوادث الأمن السيبراني في المستقبل نتيجة لإفشاء أسرار تجارية ، كما يحتفظ المديرون بالسلطة التقديرية في تحديد ماذا وكيف يتم الإفصاح عن مخاطر الأمن السيبراني.

وفي نفس الاتجاه أشار Cheong et al.(2021) إلي وجود مخاوف محتملة بشأن معلوماتية الإفصاح عن مخاطر الأمن السيبراني، وهي أن تفشل الشركات في التعرف على جميع مخاطر الأمن السيبراني التي تواجهها، أو أن تقوم الشركات بإخفاء المعلومات لتجنب المخاطر المحتملة المرتبطة بالإفصاح ، كما توجد خطورة من استغلال المهاجمين للإفصاح عن معلومات تفصيلية حول مخاطر الأمن السيبراني أو الإجراءات المضادة ، واستغلال نقاط الضعف، ومخاطر السمعة والتعويضات. وأيضاً أوضح Cheng et al.(2022) أن إفصاح الشركات عن تقرير مخاطر الأمن السيبراني، قد يفسر من جانب المستثمرون ويبرز جهود الشركة وفاعليتها في التعامل مع مخاطر الأمن السيبراني ومنع حدوث الانتهاكات، أو أن يعتقد المستثمرون أن الشركة مقصرة في إتخاذ إجراءات إضافية لتجنب حدوث خروقات أمنية.

ويخلص الباحث مما سبق إلي أن الإفصاح عن مخاطر الأمن السيبراني له أهمية ومردود يتمثل في مساعدة أصحاب المصالح في التنبؤ بإمكانية حدوث أحداث سلبية في المستقبل. وتقليل عدم التأكد، وجذب المستثمرين، وزيادة الثقة في مجهودات الشركة نحو إدارة مخاطر الأمن السيبراني. وتقليل تكاليف التقاضي المحتملة ويحسن التواصل، وبناء الثقة مع أصحاب المصالح، ولكن توجد مخاوف محتملة بشأن معلوماتية الإفصاح عن مخاطر الأمن السيبراني، واستغلال المعلومات المفصح عنها.

2-6 قرار الاستثمار في الأسهم من منظور المحاسبة المالية في بيئة تكنولوجيا المعلومات

تتمثل الوظيفة الأساسية لأسواق رأس المال في تجميع وتحويل الأموال ما بين المقرضين والمقترضين، من خلال استغلال الفرص الاستثمار المتاحة في الأسوق. كما يتعلق قرار الاستثمار بقيام المستثمر بتوجيه الأموال، بشكل مباشر أو غير مباشر بواحد أو أكثر من الأصول المادية أو المالية في الأسواق، من أجل تحقيق عائد اقتصادي بهدف تعظيم الثروة، والحفاظ على السيولة، وتقليل المخاطر (Obamuyi,2013). ويوجد نوعان من المستثمرين؛ مستثمرون مؤسسسون، وتكون طبيعة عملهم مقيدة بالقواعد واللوائح، ومستثمرون أفراد يستثمرون في الأسوق بهدف جني الأرباح، دون أن يكون رأسمالهم محدد بأي قوانين (Lutfi, 2011; Obamuyi, 2013; Miazee et al.,2014).

وفيما يتعلق بالمستثمرين الأفراد المشاركين في الأسواق المالية، لا يمكن المبالغة في التأكيد على أهمية قراراتهم الاستثمارية لأنها ترتبط مباشرًا بجودة حياتهم ، في ظل عدم توافر الموارد المالية الكافية، وافتقار معظمهم إلى المعرفة المالية الأساسية. كما تتوقف قدرة المستثمر الفرد بشكل كبير علي قدرته ومعرفته وثقته، وكذلك دقة المعلومات التي يعتمد عليها في اتخاذ القرارات (Lutfi, 2011; Miazee et al., 2014).

وتلعب تكنولوجيا المعلومات دورًا رئيسيًا اليوم في عالم الأعمال، حيث توفر مجموعة واسعة من الأدوات للشركات لتسهيل وزيادة كفاءة الأعمال. وعلى الرغم من أنها تقدم العديد من الفوائد للشركات والمستثمرون ولكنها تجلب معها أيضًا مخاطر وتهديدات أمنية وخروقات ضخمة جنبًا إلى جنب مع طبيعتها الداعمة، (D'Arcy et al., 2014; Roskot et al., 2020; Tayaksi et al., 2021; Cheong et al., 2021; Walton et al., 2021).

كما تتزايد مخاوف المستثمرين بشأن تعرض الشركات لمخاطر انتهاكات الأمن السيبراني باعتباره أحد أكبر التهديدات والتي تؤثر على استثماراتهم في الأسهم. وتعمل الشركات على زيادة الاستثمار في مواجهة الانتهاكات السيبرانية، وتعزيز عمليات الإفصاح عن إدارة الأمن السيبراني لبناء الثقة مع أصحاب المصالح، وتوفير الشفافية حول قدراتها على مواجهة مخاطر الأمن السيبراني (Bauer & Van Eeten, 2009; Spanos & Angelis, 2016; Cheong et al., 2021; Kelton, 2021).

وعلى الرغم من أن عمليات الإفصاح عن إدارة مخاطر الأمن السيبراني، توفر إشارات إيجابية للمستثمرين بشأن مخاوفهم، لتمكنهم من تحديث تقييماتهم. بحيث يتضمن سعر سهم الشركة تلك المعلومات

(Ali et al., 2021). إلا أن قرارات المستثمرين قد تكون متباينة ذات تأثير إيجابي بشأن الاستثمار في الأسهم، أو سلبي في حالة وجود انتهاكات سيبرانية (Morse et al., 2017; Roskot et al., 2020).

ويخلص الباحث مما سبق إلي أن قرار الاستثمار في الأسهم يحتاج إلي معلومات معظمها ينتجه نظام معلومات المحاسبة المالية. وأن بيئة تكنولوجيا المعلومات فرضت علي نظام معلومات المحاسبة المالية حتمية إنتاج معلومات غير مالية لخدمة المستثمرين بالأسهم، ومن أهم هذه المعلومات، معلومات عن كفاءة إدارة الشركة في إدارة مخاطر الأمن السيبراني.

6-3 تحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم واشتقاق فرض البحث الأول

أشار Chai & Rao (2011) إلي وجود رد فعل إيجابي من جانب المستثمرين بشأن اتجاه الشركات للإستثمار في الأمني السيبراني. وقد أوضح Gordon et al. (2010) أن الإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني، يمكن الشركة من تقديم إشارات إلى المستثمرين والأسواق، بشأن قدرتها علي منع الانتهاكات السيبرانية، وإكتشافها وتصحيحها في حالة حدوثها، كما أكد علي أن تزايد الإفصاح الاختياري عن مخاطر الأمن السيبراني، يرتبط بشكل إيجابي وكبير بسعر السهم، وقيمة الشركة. كما أشار Farkas & Murthy (2014) إلي أن الشركات تميل إلى الإفصاح عن المعلومات بشأن إدارة مخاطر الأمن السيبراني، نظراً لزيادة وعي أصحاب المصالح بخطورة انتهاك المعلومات، حيث يمثل اهتمامهم أحد العوامل التي تدفع الشركات للاهتمام بالأمن السيبراني.

ومن ناحية أخري أشار Goel & Shawky (2014) إلي وجود تأثير سلبي علي أسعار الأسهم بسبب إعلان الشركات عن وجود إختراق للأمن السيبراني لديها. كما أوضح Spanos & Angelis (2016) أن الأحداث المتعلقة بالانتهاكات السيبرانية ، يمكن أن تخفض من قيمة سعر سهم الشركة من 10 إلى 25٪.

وقد اتجه Morse et al. (2017) لاختبار أثر إفصاح الشركات الأمريكية عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين، وذلك بعد الإرشادات والتوجيهات التي تم إصدارها من جانب SEC في عام 2011، إلا أنه توصل لعدم وجود علاقة ذو دلالة إحصائية لإفصاح الشركات عن مخاطر الأمن السيبراني، علي قرارات المستثمرين.

كما أوضح Islam et al.(2018) أن المستثمرين يترددون في الإستثمار في الشركات التي لها تاريخ من التعرض للهجمات السيبرانية.

ويري(2019)Perols أن المستثمرين لديهم تصورات وقرارات أكثر مصداقية للاستثمار في الشركات، التي تفصح اختيارياً عن إدارة مخاطر الأمن السيبراني لديها بشكل منفصل، وفي ظل وجود مراجعة جيدة، وأن هذا لا يعد منعاً لوقوع حوادث سيبرانية في المستقبل، ولكن يعد بمثابة مؤشراً للقدرة علي التعافي من الحوادث في حالة حدوثها. كما أن المستثمرين يكونون أقل رغبة في الاستثمار عندما يتم إدارة مخاطر الأمن السيبراني بشكل مشترك، مقارنة بالقضايا التي يتم إدارتها بشكل منفصل.

وقد وجد Cheng & Walton (2019) أن مبادرة الإفصاح عن إدارة مخاطر الأمن السيبراني تؤثر على أحكام المستثمرين غير المحترفين، حيث تؤدي إفصاحات الشركة التى تم انتهاكها إلى انخفاض الرغبة في الاستثمار من جانب المستثمرين غير المحترفين وتؤثر علي أحكامهم وقراراتهم الاستثمارية. وقد خلص Yang et al. (2020) إلي أن المستثمرين غير المحترفين يدركون الفوائد من الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وهو ما يظهر في التاثير الإيجابي علي وعيهم وتصورهم وثقتهم نحو الاستثمار.

كما أكد Szubartowicz & Schryen (2020) علي أن سعر السهم يتأثر بشكل إيجابي بإعلان الشركة عن استثماراتها في الأمن السيبراني. أيضاً أكد Kelton & Pennington (2020) علي أن الإفصاح عن إدارة مخاطر الأمن السيبراني لها تأثير ايجابي علي قرارات المستثمرين غير المحترفين. وتوصل(Walton et al., 2021) إلي وجود ارتباط إيجابي بين الإفصاح عن إدارة الأمن السيبراني وجاذبية الاستثمار.

وأكد Kelton (2021) علي أن الشركات تسعي لتعزيز عمليات الافصاح عن إدارة مخاطر الأمن السيبراني لزيادة ثقة أصحاب المصالح وتوفير الشفافية حول قدرتهم على منع واكتشاف حوادث الأمن السيبراني والاستجابة لها.

وقد أشار Tosun(2021) إلي أن الإفصاح عن أحداث الاختراق الإلكتروني يؤثر علي سمعة الشركات وأداء السوق حتى خمس سنوات بعد إعلان الخرق الأمني، بسبب زيادة الإهتمام من جانب المستثمرين. وكذلك أكد Kamiya et al. (2021) أن الهجمات السيبرانية لها تأثير سلبي علي سمعة الشركة وأسعار أسهمها، وتقييم الشركة من جانب أصحاب المصالح.

وأوضح Ali et al. (2021) أن المستثمرين يعاقبون الشركات المخترقة بشدة خصوصاً عندما تكون منتمية لصناعة الإنترنت والتكنولوجيا.

كما أوضح Cheng et al. (2022) أن المستثمرين غير المحترفين يتأثرون بإفصاح الشركات عن مخاطر الأمن السيبراني، وأنهم يكونون أقل اتجاهاً ورغبة للاستثمار في الشركات التي تم اختراقها سابقاً،

إلا أن الإفصاح عن مخاطر الأمن السيبراني يؤدي إلى التخفيف من الأثر السلبي لأخبار الاختراق الأمني.

ويري(2022) D'Arcy & Basoglu أن أصحاب المصالح يسعون للحصول على المعلومات من الشركات بشأن أمنها السيبراني، فأكثر من 70٪ من المستثمرين الأمريكيين مهتمون بممارسات الأمن السيبراني للشركات للمساعدة في إتخاذ قراراتهم الاستثمارية، وكذلك يدفع المنظمون الشركات للإفصاح عن المزيد من معلومات الأمن السيبراني التي من شأنها تكون مفيدة للمستثمرين وغيرهم من المشاركين في السوق، مثل؛ وكالات التصنيف الائتماني والمحللين الماليين، نظراً لحاجاتهم لمعلومات بشأن تقييم أداء الشركة وقدرتها على البقاء على المدى الطويل. كما يري (2022) Masoud & Al-Utaibi أن الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية قبل وبعد حوادث الأمن السيبراني. يعد أمرًا إيجابيًا وهامًا.

ومنهجياً، اتبعت الدراسات السابقة مداخل مختلفة عند تناولها للعلاقة بين الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات المستثمرين ما بين مدخل تحليل المحتوي، والمدخل النظري التحليلي، والمدخل التجريبي، إلا أن كثير منها غلب عليها الطابع التجريبي عند تناولها للعلاقة محل الدراسة مثل (Perols, 2019; Frank et al., 2019; Cheng & Walton, 2019; Cheng et al., 2022; Kelton & Pennington, 2020; Yang et al., 2020). وعلي الرغم من اختلاف المنهجية المستخدمة إلا أن الدراسات في غالبيتها اتفقت علي التأثير الايجابي لإفصاح الشركات عن إدارة مخاطر الامن السيبراني علي قرارات المستثمرين. وفيما يتعلق **بالبيئات** التي أجريت فيها الدراسات، فقد تمت أغلبها في بيئات دول متقدمة، مثل، الولايات المتحدة الأمريكية، ومنها (Perols, 2019; Kelton & Pennington, 2020; Yang et al., 2020; D'Arcy & Basoglu, 2022; Masoud & Al-Utaibi, 2022). وبعضها في دول نامية مثل الصين Kamiya et al. (2021) وهو ما يفسر إهتمام كل من الدول المتقدمة والنامية بالأمن السيبراني وتأثيره علي قرارات أصحاب المصالح وخاصة المستثمرين.

ويخلص الباحث مما سبق إلي أن اتجاه الشركات للإفصاح عن المعلومات حول إدارة مخاطر الأمن السيبراني، بسبب زيادة وعي أصحاب المصالح وخاصة المستثمرين، بخطورة انتهاك المعلومات، وأيضاً لزيادة الثقة وتوفير الشفافية حول قدرة الشركة على منع واكتشاف الحوادث السيبراني والاستجابة لها والتعافي منها. **كما يخلص الباحث إلي** أن الإفصاح عن إدارة مخاطر الأمن السيبراني يؤثر بشكل إيجابي على قرارات المستثمرين غير المحترفين، ويزيد من ثقتهم في الاستثمار. كما أنهم يتأثرون بالمعلومات حول الانتهاكات السيبرانية والتي تقلل من رغبتهم في الاستثمار، كما أن الإفصاح عن اختراق الأمن السيبراني يؤثر سلباً علي سمعة الشركات وأسعار أسهمها، وأن الإفصاح عن مخاطر الأمن السيبراني يعد أمرًا هامًا.

ويري الباحث أن في ظل التطور التكنولوجي وعصر المعرفة، تتجه الشركات للاستثمار في الأمن السيبراني، لمواجهة حالات اختراق نظام المعلومات، وأن إفصاحها عن برنامج إدارة مخاطر الأمن السيبراني، يكون بغرض إعطاء إشارات إيجابية للمستثمرين، لكسب ثقتهم وإهتمامهم ، وجذبهم وزيادة رغبتهم للاستثمار في الشركة وهو ما يعد أمرًا هامًا.

وبُناء علي ما سبق يتوقع الباحث أن يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين. ونظراً لندرة الدراسات المصرية العملية في هذا المجال بالإضافة لغياب الممارسة العملية فلن يتبني الباحث اتجاهاً معيناً لهذه العلاقة. ولذا يمكن اشتقاق الفرض الأول (H1) علي النحو التالي:

H1: يؤثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين.

6-4 تحليل أثر السمات النوعية والفنية للمستثمرين المصريين غير المحترفين علي العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارهم بالاستثمار في الأسهم وإشتقاق فروض البحث من الثاني حتي الخامس

أشار كل من (Mohebzada et al., 2012; Yan et al., 2018; Fatokun et al., 2019) إلي أن سمات المستثمرين النوعية والفنية تعتبر من المؤشرات التي يمكن أن يُستند إليها في تفسير الاختلافات في سلوك المستثمرين وتفضيلاتهم وقراراتهم الاستثمارية. **وسوف يتناول الباحث بعض من هذه السمات مثل؛(نوع جنس المستثمر، العمر، مستوي التأهيل العلمي) ومدي تأثيرها علي العلاقة محل الدراسة، وذلك كما يلي:-**

6-4-1 تحليل أثر اختلاف نوع جنس المستثمر علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين واشتقاق الفرض الثاني للبحث(H2)

أشار Pompian & Longo (2004) إلي أن كلا الجنسين لديهما معتقدات وتحيزات سلوكية ومالية مختلفة عن الأخر. وقد أوضح Wood & Zaichkowsky (2004) أن المستثمرات النساء أكثر تحفظًا من الرجال عند اتخاذهم لقرار الاستثمار، ويعتمدن أكثر على الوسطاء الماليين، لتقليل خطورة قرارتهم الاستثمارية، بينما المستثمرون الرجال لديهم مستوى ثقة أعلى وتحمل للمخاطر من المستثمرات النساء عند اتخاذ قرارا الاستثمار. كما توصل Hira & Loibl (2008) إلي وجود اختلافات في سلوك المستثمرين

ترجع للاختلاف في جنس المستثمر. كما يوضح(2015)Mishra & Metilda أن درجة الثقة المرتبطة بقرار الاستثمار تختلف ما بين النساء والرجال، فتكون أعلى بين الرجال منها لدى النساء وتزداد مع خبرة الاستثمار والتعلم.

وقد اتجه (2011) Lutfi لاختبار العلاقة بين مجموعة من العوامل ومنها، جنس المستثمر وسلوكه من جه وقراره من جه أخري، وأوضح أن المستثمرين الرجال ينفقون المزيد من الوقت والمال في دراسة فرص الاستثمار، والاعتماد بشكل أقل على الوسطاء الماليين، بالإضافة إلى أن المستثمرات النساء أكثر تردداً نحو اتخاذ قرار الاستثمار، كما أن المستثمرين الرجال أكثر ثقة وتقبلاً لمخاطر الاستثمار في الأسهم. ممايعني وجود علاقة بين جنس المستثمر وقرار الاستثمار. كما يري (2012) ,Jain & Mandot أن السمات مثل، العمر والحالة الاجتماعية، والجنس، ومستوى الدخل، والخبرة بالسوق تؤثر على قرار المستثمر. في حين اختبر(2017) .Anwar et al إلى أي مدى يلعب اختلاف الجنس دورًا في التأثير على معتقدات وسلوكيات الأفراد بشأن الأمن السيبراني ، وتوصل إلي أن اختلاف الجنس له تأثير بارز فيما يتعلق بالخبرة السابقة ، والكفاءة الذاتية وسلوكيات الأمن السيبراني فالنساء لديهن انخفاض في الكفاءة الذاتية عن الرجال فيما يتعلق بالأمن السيبراني. كما أشار(2018) .Gratian et alإلي أن جنس المستثمر وسماته الشخصية، وتفضيلات المخاطرة، تعد من العوامل الهامة للتنبؤ بسلوكه وقراراته المتعلقة بالأمن السيبراني.

وفي نفس الاتجاه استهدف (2019).Fatokun et al اختبار ما إذا كان يوجد اختلافات في معتقدات وسلوكيات المستثمرين الأفراد فيما يتعلق بالأمن السيبراني باختلاف جنس المستثمر، وتم إجراء دراسة علي عينة من340 من طلبة الدراسات العليا في إحدي الجامعات بماليزيا ، وتوصل إلي أن سلوكيات الأمن السيبراني وقدرة الطلاب علي الإلمام بالتهديدات السيبرانية وفعالية الاستجابة تختلف بناءً على عدة عناصر منها جنس المستثمر، حيث يكون لها بعض التأثيرات على تصورات وقرارات وسلوكيات الطلاب تجاه مخاطر الأمن السيبراني. فيما توصل(2022) Radu & Smaili لوجود علاقة إيجابية معنوية بين مستوى الإفصاح عن الأمن السيبراني والتنوع بين الجنسين في مجلس الإدارة، ويري أنه إذا كان المستثمرون يرغبون في زيادة الإفصاح عن معلومات متعلقة بإدارة الأمن السيبراني، فعليهم أن يطلبوا المزيد من المجالس المتنوعة، وزيادة تمثيل المرأة في مجالس الإدارة.

ويخلص الباحث مما سبق إلي وجود اختلاف بين الجنسين فيما يتعلق بمعتقدات ومستوي الثقة وتقبل المخاطر المرتبطة بقرار الاستثمار. وأن عامل نوع جنس المستثمر يؤثر علي سلوكه ومعرفته عند اتخاذه للقرارات. وكذلك يؤثر نوع الجنس علي كفاءة ومعتقدات وتصورات وسلوكيات المستثمرين الأفراد غير

المحترفين بشأن الأمن السيبراني. وأيضاً وجود علاقة بين مستوى الإفصاح والتنوع بين الجنسين في مجلس الإدارة.

ويري الباحث أن عامل نوع جنس المستثمر هو أمر مهم ومؤثر في السلوكيات البشرية بشكل عام. ومن الطبيعي أن يختلف المستثمرون في قراراتهم وفقاً لجنسهم والذي يؤثر علي معتقداتهم وتصوراتهم ورغبتهم الاستثمارية. وبالتالي قد يختلف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين باختلاف نوع المستثمر.

وبُناء علي ما سبق يتوقع الباحث أن يختلف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر. ولذا يمكن اشتقاق الفرض الثاني للبحث (H2) علي النحو التالي:

H2: يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر.

6-4-2 تحليل أثر اختلاف العمر علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين واشتقاق الفرض الثالث للبحث(H3)

أشار Lutfi (2011) إلي وجود علاقة معنوية بين عمر المستثمر وسلوكه المتعلق بتحمل مخاطر الاستثمار واختياره لنوع الاستثمار. كما وجد Menkhoff et al. (2013) أن خبرة المستثمر وعمره لها تأثير كبير على مستوى ثقته وقراراته الاستثمارية.

وقد أوضح Mohebzada et al.(2012) أن العمر والجنس والمستوى التعليمي لهما بعض التأثيرات عل قدرة الأفراد علي مواجهة التهديات الالكترونية، فالأقل من عمر 21 عام أقل قدرة علي مواجهة التهديدات السيبرانية. بينما توصل Arachchilage, & Love (2014) إلي أنه كلما كان العمر أصغر، زادت قابلية القدرة علي مواجهة تلك التهديات الالكترونية.

وبشأن الفروق الفردية المتعلقة بسلوكيات التعامل مع مخاطر الأمن السيبراني، توصل Whitty et al. (2015) إلي أن بعض العوامل مثل عمر الفرد، يعد من بين أمور أخرى، تمثل مؤشرا هاماً ومتعلق بسلوك الأفراد بشأن التعامل مع التهديدات السيبرانية. كما أوضح Chakraborty et al. (2016) في دراسة أجريت علي طلاب جامعيين في إحدى الجامعات الأمريكية، أن الطلاب الأكثر عمراً لديهم تصورات تتعلق بالتهديدات الالكترونية أكبر من غيرهم من الأقل عمراً، علي الرغم من أن معظم الطلاب الجامعيين كانوا ليس على دراية كافية بالعديد من التهديدات الإلكترونية.

كما بين Öğütçü et al.(2016) أن الفئات العمرية الأدنى أكثر عرضة للهجمات الإلكترونية. وقد توصل Jeske & Van Schaik (2017) إلي أن الأفراد الأصغر سنًا أقل إلمامًا بالتهديدات الإلكترونية على عكس الأكبر سناً، مما يدل على اختلافهم في إلمامهم بالتهديدات الإلكترونية على أساس العمر. وقد دعي Yan et al.(2018) لإجراء مزيد من الاختبارات حول كيفية تأثير العمر والجنس والمستوى التعليمي على سلوكيات التعامل مع الأمن السيبراني.

ويخلص الباحث مما سبق إلي أن عمر المستثمر يعد من بين أمور أخرى تؤثر علي سلوكه ومستوى ثقته وتصوراته وقراراته الاستثمارية، وقدرته علي مواجهة التهديات السيبرانية، مما يعني وجود على اختلاف في إلمامهم بالتهديدات الإلكترونية على أساس العمر.

ويري الباحث أن عمر المستثمرين الأفراد تعد من بين الأمور التي يعتقد أن تؤثر علي مستوي تفكيره ومعتقداته وخبرته ودرجة تقبله للمخاطر، وكيفية تعامله مع التهديدات السيبرانية، ودرجة المامه واستيعابة للمعلومات التي تفصح عنها الشركات والمتعلقة بالأمن السيبراني.

وبُناء علي ما سبق يتوقع الباحث أن يختلف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف العمر. ولذا يمكن اشتقاق الفرض الثالث للبحث (H3) علي النحو التالي:

H3: يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف العمر.

6-4-3 تحليل أثر اختلاف مستوي التأهيل العلمي علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين واشتقاق الفرض الرابع للبحث(H4)

اتفق (Schooley & Worden, 1999; Bhandari & Deaves, 2006) علي أن المستثمرين الذين يتلقون مستوي مرتفع من التعليم لديهم من المعرفة والمهارات التي تفيدهم في اتخاذ قرارات الاستثمار، ويكونون أكثر ثقة من الذين لديهم مستوى تعليمي منخفض، كما أنهم يكون متقبلون للمخاطر بشكل أكبر من غيرهم. كما أكد Deaves et al. (2010) أن ثقة المستثمر تزداد مع ارتفاع مستوي تعليمه. وأيضاً اتفق(Lutfi, 2010; Obamuyi, 2013) علي أن المستثمر الذي يرتفع لدية مستوي التعليم تزداد لدية المعرفة والمهارة التي تحسن من قدراته الاستثمارية بما ينعكس علي العائد علي الاستثمار. كما أوضح

Christanti & Mahastanti (2011) أن المستوي التعليمي وخبرة المستثمر يؤثران علي مستوي الاستثمار في الأسهم.

كما أشار Miazee & Hasan(2014) إلي أن المستثمرين المؤهلين علمياً لديهم المعرفة والمهارة التي تمكنهم من إتخاذ القرارات الاستثمارية بجودة مقارنة بالمستثمرين غير المؤهلين، كما أن زيادة مستوي التعليم تحسن من قدرة المستثمر علي تحمل المخاطر، وتحسن من جودة أحكامهم الاستثمارية. ويؤكد Mishra & Metilda (2015) علي أن كل من نوع وعمر وخبرة ومستوي التأهيل العلمي للمستثمر والشهادات العلمية التي يحصل عليها أصحاب المصالح تؤثر علي سلوكهم، وجودة قراراتهم الاستثمارية. وكذلك أشار Lan et al. (2018) إلي أن خصائص المستثمر مثل مستوي تأهيله العلمي وخبرته تؤثر علي سلوكه وأحكامه وقراراته الاستثمارية. وقد توصل Fatokun et al. (2019) إلي أن الفروق في المستوى التعليمي تعطي إشارات وتمكن من العمل والإلمام بالتهديدات السيبرانية، وأن خصائص العمر والجنس والمستوى التعليمي تمثل عوامل مهمة متعلقة بسلوكيات التعامل مع الأمن السيبراني.

ويخلص الباحث مما سبق إلي أن المستثمرون الذين لديهم مستوي مرتفع من التعليم ويحصلون علي شهادات مهنية يكتسبون المعرفة والمهارات التي تفيدهم وتؤثر علي جودة أحكامهم عند اتخاذ قرارات الاستثمار، ويكونون أكثر ثقة من غيرهم. وأن الاختلاف في المستوى التعليمي يظهر في التعامل مع التهديدات السيبرانية.

ويري الباحث أن ارتفاع مستوي تعليم المستثمر يحسن من قدراته ويمكنه من دراسته وفهمه للمعلومات المتعلقة بالفرص الاستثمارية، وتعاملة مع المخاطر والتهديدات السيبرانية.

وبُناء علي ما سبق يتوقع الباحث أن يختلف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر. ولذا يمكن اشتقاق الفرض الرابع (H4) علي النحو التالي:

H4: يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر.

6-4-4 تحليل أثر اختلاف كل من الجنس والعمر ومستوي التأهيل العلمي للمستثمر معاً علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين واشتقاق فرض البحث الخامس(H5)

أشارت الكثير من الدراسات (Lutfi ,2011; Shanmugsundaram & Balakrishnan,2011 ; Shaikh &Kalkundrikar, 2011; Jain & Mandot, 2012; Geetha & Ramesh, 2012; Obamuyi, 2013; Mishra & Metilda, 2015; Lan et al., 2018) إلي أن خصائص المستثمرين مثل؛ الجنس، والعمر، ومستوي التعليمي، والمؤهلات العلمية، ومستوى المعرفة والدخل، ترتبط بطريقة أو بأخرى وتفسر سلوك المستثمرين تجاه تقبلهم للمخاطر وتفضيلاتهم، وجودة قراراتهم، ويمكن استخدامها للتنبؤ بقراراتهم الاستثمار. كما أوضح (Mohebzada et al., 2012) أن كل من العمر، والجنس، والمستوى التعليمي لهما بعض التأثيرات علي قدرة الأفراد علي مواجهة التهديات السيبرانية.

وقد اتفقت بعض الدراسات(Hira & Loibl, 2008; Mishra & Metilda,2015) علي أنه يمكن إرجاع وجود اختلافات في سلوك المستثمرين، ودرجة الثقة المرتبطة بقرار الاستثمار للاختلاف في جنس المستثمر. كما أشار(Anwar et al., 2017; Gratian et al., 2018; Fatokun et al., 2019) إلي أن جنس المستثمر وسماته الشخصية، تلعب دورًا في التأثير على تصورات ومعتقدات وسلوكيات الأفراد بشأن الأمن السيبراني، وتعد من العوامل الهامة للتنبؤ بالقرار والسلوك والكفاءة الذاتية المتعلقة بالأمن السيبراني.

وأيضاً اتفق البعض (Lutfi, 2011; Menkhoff et al., 2013) علي أنه يوجد علاقة بين عمر المستثمر وسلوكه المتعلق بتحمل مخاطر الاستثمار واختياره لنوع الاستثمار ومستوى ثقته وقراراته الاستثمارية. كما توصل (Arachchilage, & Love, 2014; Whitty et al., 2015; Chakraborty et al., 2016) إلي أنه كلما كان عمر المستثمر أقل، كلما زادت قدرته علي مواجهة التهديات الالكترونية.

وكذلك اتفقت بعض الدراسات (Schooley & Worden, 1999; Bhandari & Deaves, 2006; Deaves et al., 2010; Lutfi, 2010; Obamuyi, 2013) علي أن المستثمرين المؤهلين علمياً لديهم المعرفة والمهارة التي تمكنهم من اتخاذ القرارات الاستثمارية بجودة مقارنة بغيرهم ، كما أن زيادة مستوي التعليم يحسن من قدرة المستثمر علي تحمل المخاطر، وتحسن من جودة أحكامهم الاستثمارية، كما أن ثقة المستثمر تزداد مع ارتفاع مستوي تعليمه.

ويخلص الباحث مما سبق إلي أن الدراسات أشارت لتأثير بعض العوامل مثل؛ الجنس ، والعمر، والمستوي التعليمي، والمؤهلات العلمية، علي سلوك المستثمرين تجاه تقبلهم للمخاطر وتفضيلاتهم

الاستثمارية وثقتهم وجودة قراراتهم، كما يمكن استخدامها للتنبؤ بقراراتهم الاستثمار، والتعامل مع قضايا الأمن السيبراني وقدرتهم علي مواجهة تلك التهديدات.

ويري الباحث أن كل من العمر والجنس والمستوى التعليمي قد تمثل جزء من عوامل مؤثرة علي سلوكيات المستثمرين الأفراد غير المحترفين عند تعاملهم مع المعلومات المتعلقة بالأمن السيبراني.

وبُناء علي ما سبق يتوقع الباحث أن يختلف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف كل من الجنس والعمر ومستوي التأهيل العلمي للمستثمر معاً. ولذا يمكن اشتقاق الفرض الخامس (H5) علي النحو التالي:

H5: يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف كل من الجنس والعمر ومستوي التأهيل العلمي للمستثمر معاً.

6-5 منهجية البحث

يستهدف الباحث في هذه الجزئية عرض منهجية البحث تمهيداً لإختبار فروضه تجريبياً. وفي سبيل تحقيق هذا الهدف سيعرض الباحث لكل من؛ أهداف الدراسة التجريبية ومجتمع وعينة الدراسة، وتوصيف وقياس متغيرات الدراسة، وأدوات وإجراءات الدراسة التجريبية، ونموذج البحث، والتصميم التجريبي المستخدم، والمعالجات التجريبية، والمقارنات بين المعالجات، والأساليب الإحصائية المستخدمة لتحليل نتائج الدراسة التجريبية، وأخيرا نتائج إختبار فروض البحث، وذلك علي النحو التالي:

6-5-1 أهداف الدراسة التجريبية

تستهدف الدراسة التجريبية، إختبار فروض البحث، لقياس ما إذا كان هناك تأثير لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، وذلك قياسًا على (Cheng & Walton, 2019; Perols, 2019; Frank et al., 2019; Kelton & Pennington, 2020; Kelton, 2021; Cheng et al., 2022)

6-5-2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من المستثمرين المصريين غير المحترفين[1]. وقد قام الباحث بتوزيع الحالات الافتراضية على العينة[2] من المجتمع، كما موضح بالجدول رقم (1)، وذلك قياسًا على (Obamuyi, 2013; Cheng & Walton, 2019; Perols, 2019; Frank et al., 2019; Kelton & Pennington, 2020; Kelton, 2021; Cheng et al., 2022)

جدول 1: بيان بالحالات التجريبية الموزعة على عينة الدراسة

عينة الدراسة / العدد	المستثمرين غير المحترفين
الحالات الموزعة	135
الحالات المستلمة	115
نسبة الاستجابة	%85
الحالات الصحيحة	108 [3]

[1] إعتمد الباحث في إجراء الدراسة التجريبية علي المستثمرين غير المحترفين لأنهم يشكلون جزءًا كبيرًا من سوق الأوراق المالية، كما يعتقد أن المستثمرين غير المحترفين قد يتفاعلون مع الإفصاح عن إدارة الأمن السيبراني، ولكن عندما تكون الشركة هي أول من يفصح عن ذلك، ويأخذون في الاعتبار المخاوف بشأنها عند إصدار أحكام الاستثمار، وذلك وفقاً (Cheng & Walton, 2019;Cheng et al.,2022).

[2] اعتمد الباحث علي عينة من أعضاء هيئة التدريس بالجامعات المصرية المختلفة، وطلاب الدراسات العليا(الدبلوم والماجستير والدكتوراه بكلية التجارة جامعة دمنهور)، ويعتقد الباحث أن لديهم المعرفة والخبرة الكافية لقراءة المعلومات المالية، والعمل كممثلون مناسبون للمستثمرون غير المحترفون، وذلك قياساً علي (Obamuyi ,2013; Fatokun et .al.,2019; Perols, 2019) وكان ما يقرب من 44% من المشاركين من الإناث، 56% من الرجال وكان عمر المشاركون في المتوسط 36 سنة وفقاً لمتوسط عمر العينة.

[3] تم استبعاد عدد من الحالات لعدم اتساق أو صدق، أو اكتمال الإجابات.

6-5-3 توصيف وقياس متغيرات الدراسة

تم توصيف وقياس متغيرات الدراسة، على النحو التالي:

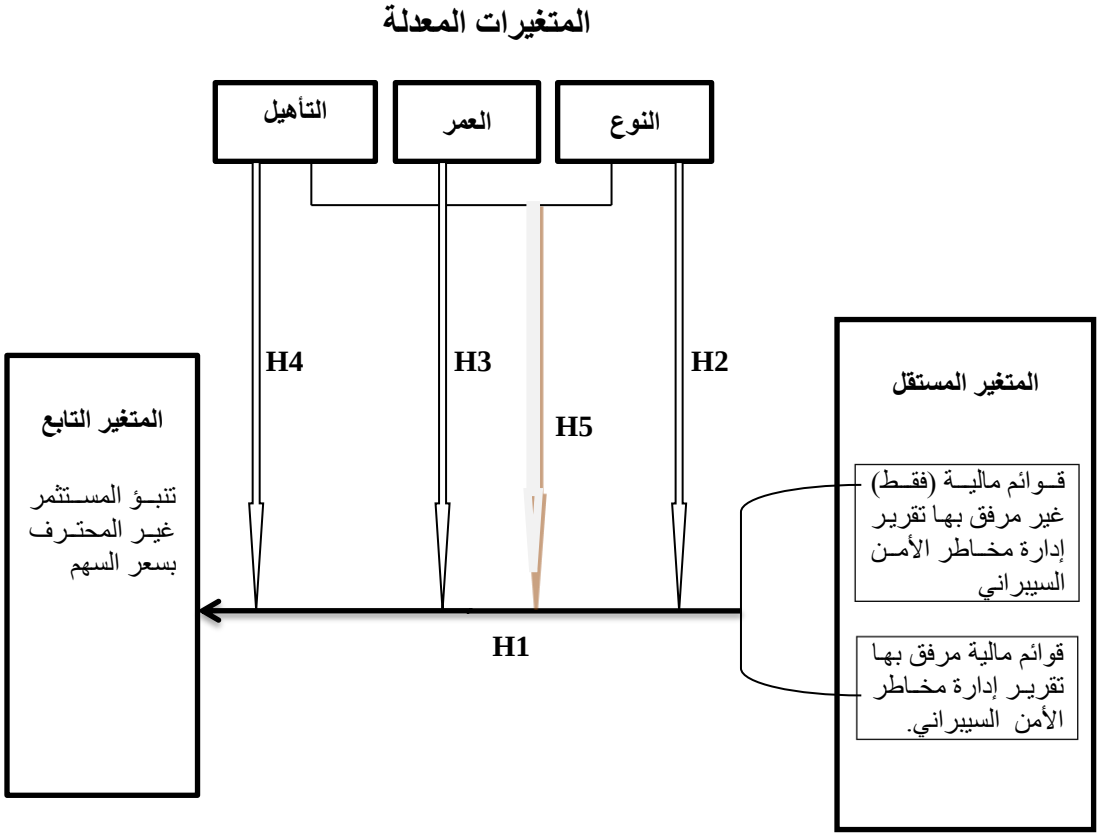
المتغير	نوعه	التوصيف وطريقة القياس	العلاقة المتوقعة
1- الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني	**مستقل**	ويعني قيام إدارة الشركة بالإفصاح عن معلومات بشأن تصميمها وتنفيذها لمجموعة من السياسات والعمليات والإجراءات الرقابية والضوابط لحماية معلوماتها وأنظمتها الإلكترونية من الأحداث والتهديدات السيبرانية والتي يمكن أن تعوق تحقيق أهدافها (AICPA, 2017; Frank et al., 2019). وتم قياسه من خلال إمداد أفراد العينة من المستثمرين المصريين غير المحترفين بقوائم مالية مرفق بها تقرير الإدارة بشأن مخاطر الأمن السيبراني، مقارنة بقوائم مالية (فقط) بدون تقرير إدارة مخاطر الأمن السيبراني قياساً علي (علي وصالح، 2021 ;Kelton & Pennington, 2020) Kelton, 2021;Cheng et al.,2022)	+ أو –
2- قرارات المستثمرين غير المحترفين	**تابع**	ويعني مدي رغبة وإستعداد المستثمرين غير المحترفين بالاستثمار في أسهم الشركة، من خلال قرارهم بالاختيار بين البدائل المتاحة، وتوقعهم لسعر السهم (علي وصالح، 2021 ;Cheng & Walton, 2019; Frank et al., 2019; Kelton & Pennington, 2020; Kelton, 2021; Cheng et al., (2022. ويتم قياسها من خلال الأسئلة الموجهة لهم المرافقة للحالة التجريبية وتوقعهم لسعر السهم في نهاية الفترة واتخاذ قرار بالاستثمار في السهم، وذلك قياساً علي (علي وصالح، 2021 (Kelton & Pennington, 2020; Cheng, et al., 2022).	
3- نوع جنس المستثمر	**معدل**	ويعني جنس المستثمر رجل أو أنثي، وتم قياسه، كمتغير يأخذ القيمة (1) إذا كان نوع جنس المستثمر رجل، ويأخذ القيمة (صفر) إذا كانت جنس المستثمر من النساء ، وذلك قياسا علي (Anwar et al., 2017).	+ أو -
4- عمر المستثمر	**معدل**	ويعني سنوات عمر المستثمر، وتم قياسه كمتغير يأخذ القيمة (1) إذا كان عمر المستثمر أكبر من متوسط عمر العينة، ويأخذ القيمة (صفر) إذا كان يساوي أو أقل من متوسط عمر العينة قياساً علي (Lutfi, 2011).	+ أو -
5- مستوي التأهيل العلمي للمستثمر	**معدل**	ويعني المستوي التعليمي والمؤهلات العلمية، والشهادات المهنية ، التي حصل عليها المستثمر، والتي تعمل علي زيادة المعرفة والمهارة، وتحسن من قراراته الاستثمارية (Lutfi, 2010; Obamuyi, 2013). وتم قياسه كمتغير يأخذ القيمة (1) إذا كان المستثمر ذو تأهيل علمي مرتفع، من خلال حصولة علي درجات عليا مثل درجة الدكتوراه أوشهادات مهنية، ويأخذ القيمة (صفر) خلاف ذلك، وكان المستثمر ذو تأهيل علمي منخفض(علي وصالح، 2021).	+ أو -

6-5-4 أدوات وإجراءات الدراسة

تم اجراء الدراسة التجريبية قياساً علي منهجية (Cheng & Walton, 2019; Kelton & Pennington, 2020; Cheng et al., 2022). وتتمثل أدواتها في الحالات الافتراضية التجريبية والأسئلة المرافقة لها[1]. وقد تم إعداد هذه الحالات لقياس مدي تأثير إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. وقد قام الباحث بتصميم الحالة الافتراضية التجريبية، والتى اشتملت على ثلاثة أقسام؛ **يتعلق القسم الأول؛** بالبيانات الشخصية لمفردات عينة الدراسة. **ويتضمن القسم الثاني؛** بعض المصطلحات الفنية ذات الصلة. وأخيراً **القسم الثالث،** ويشتمل علي الحالات التجريبية.

وتتضمن الحالة التجريبية الأولي؛ ملخصاً للقوائم المالية لإحدى الشركات الإفتراضية، لسنتين 2020 ، 2021، والتي تم مراجعتها، بالإضافة لبعض الإيضاحات المتممة عن السنة المنتهية في2021/12/31، وسعر إقفال سهم الشركة في نهاية عامي 2020، و2021. وقد تضمنت هذه الحالة سؤالين؛ في السؤال الأول طُلب من مفردات العينة تحديد مدي رغبتهم في الاستثمار في أسهم هذه الشركة، وتم تخصيص القيمة (0) للإجابة "**لا أرغب بالمرة**" إلي القيمة (10) للإجابة" **أرغب تماما**"، والهدف من ذلك تحديد مدي رغبتهم في الاستثمار في أسهم هذه الشركة وذلك قياساً علي(Cheng & Walton, 2019). والسؤال الثاني يتعلق بتوقعهم لسعر اقفال أسهم الشركة في 2022/12/31. ثم تم الانتقال للحالة التجريبية الثانية، والتي تتضمن نفس معلومات الحالة التجريبية الأولي، بالإضافة لتقرير إدارة الشركة عن إدارة مخاطر الأمن السيبراني لعام 2021 والذي تم الإفصاح عنه ضمن مرفقات القوائم المالية. وقد طُلب من مفردات العينة الإجابة على نفس سؤالين الحالة التجريبية الأولي، والهدف من ذلك تحديد مدي تأثير إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات مفردات العينة عند اتخاذ قرارات الاستثمار وذلك قياساً علي (Cheng & Walton, 2019; Kelton & Pennington, 2020; Cheng et al.,2022). وتم تصميم القائمة باستخدام تقنية Google Forms وإرسالها بالبريد الالكتروني، وتم جمع الردود من المشاركين في الدراسة التجريبية، وفرزها تمهيدا لتحليلها احصائياً.

[1]– ملحق البحث رقم (1)



ويوضح الشكل 1: عرضاً لنموذج البحث

نموذج البحث: من إعداد الباحث

6-5-5 التصميم التجريبى المستخدم

لإختبار فروض البحث تم استخدام تصميم تجريبي (2×3×2) ، وذلك كما يلي:

سمات المستثمر / بدائل الإفصاح	سمات المستثمر النوعية					
	النوع		العمر		التأهيل العلمي	
	ذكر	أنثي	العمر< متوسط عمر العينة	العمر≥ متوسط عمر العينة	مؤهل	غير مؤهل
قوائم مالية (فقط) بدون تقرير إدارة مخاطر الأمن السيبراني.	المعالجة (1) التنبؤ بسعر السهم	المعالجة (2) التنبؤ بسعر السهم	المعالجة (3) التنبؤ بسعر السهم	المعالجة (4) التنبؤ بسعر السهم	المعالجة (5) التنبؤ بسعر السهم	المعالجة (6) التنبؤ بسعر السهم
قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني.	المعالجة (7) التنبؤ بسعر السهم	المعالجة (8) التنبؤ بسعر السهم	المعالجة (9) التنبؤ بسعر السهم	المعالجة (10) التنبؤ بسعر السهم	المعالجة (11) التنبؤ بسعر السهم	المعالجة (12) التنبؤ بسعر السهم

6-5-5-1 المعالجات التجريبية

تحتوي التجربة على أثنتي عشرة معالجة، على النحو التالي:

المعالجة(1): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر ذكر/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(2): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر أنثي/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(3): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ عمر المستثمر أكبر من متوسط عمر العينة/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(4): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ عمر المستثمر أقل من أو يساوي متوسط عمر العينة / ويطلب منه التنبؤ بسعر السهم.

المعالجة(5): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر مؤهل/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(6): قوائم مالية بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر غير مؤهل/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(7): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/ مستثمر ذكر/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(8): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/ مستثمر أنثي/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(9): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/عمر المستثمر أكبر من متوسط عمر العينة / ويطلب منه التنبؤ بسعر السهم.

المعالجة(10): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/عمر المستثمر أقل من أو يساوي متوسط عمر العينة / ويطلب منه التنبؤ بسعر السهم.

المعالجة(11): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/ مستثمر مؤهل/ ويطلب منه التنبؤ بسعر السهم.

المعالجة(12): قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني/ مستثمر غير مؤهل/ ويطلب منه التنبؤ بسعر السهم.

6-5-5-2 المقارنات التجريبية

ويتم إجراء عدد من المقارنات بين المعالجات، لإختبار فروض البحث على النحو التالى:

المقارنة الأولي:[(1+2+3+4+5+6)]×[(7+8+9+10+11+12)] : وذلك لقياس تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين بشأن التنبؤ بسعر السهم، **وذلك لاختبار الفرض الأول (H1).**

المقارنة الثانية:[(1×7)]×[(2×8)] : وذلك لقياس مدي اختلاف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين بشأن التنبؤ بسعر السهم باختلاف نوع جنس المستثمر، **وذلك لاختبار الفرض (H2).**

المقارنة الثالثة:[(3×9)]×[(4×10)]: وذلك لقياس مدي اختلاف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين بشأن التنبؤ بسعر السهم باختلاف عمر المستثمر، **وذلك لاختبار الفرض (H3).**

المقارنة الرابعة:[(5×11)]×[(6×12)]: وذلك لقياس مدي اختلاف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين بشأن التنبؤ بسعر السهم باختلاف مستوي التأهيل العلمي المستثمر، **وذلك لاختبار الفرض (H4).**

المقارنـة الخامسـة:[(1+3+5)×(7+9+11)]×[(2+4+6)×(8+10+12)]:وذلك لقياس مدي اختلاف تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين بشأن التنبؤ بسعر السهم باختلاف الأثر المجمع لكل من نوع جنس المستثمر، وعمره، ومستوي تأهيله العلمي، **وذلك لاختبار الفرض (H5).**

6-5-6 أدوات التحليل الإحصائي المستخدمة في اختبار فروض البحث وتحليل نتائج الدراسة التجريبية

اعتمد الباحث على عدد من الأدوات الإحصائية المختلفة لتحليل البيانات. وقد تم استخدام برنامج SPSS الإصدار رقم (22). حيث استخدم الإختبارات الإحصائية التي تتفق مع طبيعة بيانات الدراسة التجريبية، وفروض البحث، وتم الاعتماد على الأساليب الإحصائية التالية:

6-5-6-1 مقياس الاعتمادية (الثبات) Reliability

يتم استخدام مقياس Cronbach's Alpha لقياس صدق وثبات الأسئلة الخاصة بالحالات الإفتراضية التجريبية، وإختبار مدي ثبات إستجابات مفردات العينة على الأسئلة، ومدى صلاحية البيانات للتحليل الإحصائي، لبيان مدي إمكانية تعميم نتائج العينة على مجتمع الدراسة (عزام وزغلول، 2006). وكانت نتيجة الاختبار، جدول رقم(2) أن معامل قيمة Cronbach's Alpha (0.744) وهو ما يمثل مقياساً جيداً للصدق والثبات، مما يعني إمكانية تعميم النتائج.

جدول 2: Reliability Statistics

Cronbach's Alpha	N of Items
.744	4

وسوف يقوم الباحث بالاعتماد علي اختبار ويلكوكسون **Wilcoxon Signed Rank Test**، ويمثل أحد الاختبارات اللامعلمية، ويستخدم في حالة أن تكون البيانات ليست موزعة توزيعًا طبيعيًا، ويعتمد على حساب الوسيط المتوقع Expected Median لكل سؤال من الأسئلة، ويناسب هذا الاختبار في حالة وجود عينة واحدة، أو في حالة عينتين غير مستقلتين من المجموعات التجريبية (عزام و زغلول، 2006).

6-5-7 اختبار فروض البحث (التحليل الأساسي)

يعرض الباحث نتائج اختبار فروض البحث، علي النحو التالي:

6-5-7-1 نتيجة اختبار الفرض الأول (H1)

استهدف الفرض الأول(H1) اختبار ما إذا كان إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني يؤثر معنوياً علي قرارات المستثمرين المصريين غير المحترفين. واستخدم الباحث اختبار ويلكوكسون، من أجل اختبار هذا الفرض، **ولاختبار هذا الفرض تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يؤثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين. وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

وعند مستوي ثقة (1-α) 95% ودرجة خطأ (α) 5%، فإذا كانت قيمة P-Value أقل من (5%) يتم رفض فرض العدم، ومن ثم قبول الفرض البديل. أما إذا كانت قيمة P-Value أكبر من أو يساوي (5%) لا يتم رفض فرض العدم.

ويظهر الجدول التالى، (3)، (4) نتيجة اختبار الفرض الأول (H1):

Wilcoxon Signed Ranks Test

جدول3: Ranks

		N	Mean Rank	Sum of Ranks
NonSybs - WiSybs	Negative Ranks	34[a]	19.01	646.50
	Positive Ranks	2[b]	9.75	19.50
	Ties	18[c]		
	Total	54		

a. NonSybs < WiSybs
b. NonSybs > WiSybs
c. NonSybs = WiSybs

جدول 4: Test Statistics[a]

	NonSybs - WiSybs
Z	-4.992-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

يتضح من جدول رقم (4)، ووفقاً لاختبار ويلكوكسون كانت قيمة P–Value (0.000) أقل من (5%)، **وبالتالي يتم رفض فرض العدم وقبول الفرض البديل(H1). القائل بوجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين.**

وتتفق هذه النتيجة مع ما توصلت إليه دراسات (Cheng & Walton., 2019; Kelton & Pennington, 2020; Yang et al., 2020; Cheng et al., 2022) والتي ترى أن إتجاه الشركات للإفصاح عن المعلومات حول إدارة مخاطر الأمن السيبراني، يؤثر على قرارات المستثمرين غير المحترفين، حيث يوفر لهم المعلومات، التي تزيد من وعي وثقة المستثمرين، بشأن المخاطر السيبرانية التي تواجهها، لذلك فإن الإفصاح عن مخاطر الأمن السيبراني يعد أمرًا هامً.

وبالنظر إلي جدول(3)، (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب كانت أكبر في حالة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني والذي يساوي (19.01)، بالمقارنة متوسط الرتب في حالة عدم الإفصاح، والذي يساوي (9.75).

وفيما يتعلق برغبة المستثمرين في الإستثمار في أسهم هذه الشركة، في حالة الإفصاح عن تقرير مخاطر الأمن السيبراني مقابل عدم الإفصاح، فقد تم تحليل ردود المستثمرين، ووفقًا لاختبار ويلكوكسون جدول رقم (6) كانت قيمة P–Value (0.000) أقل من (5%)، **بمعنى** أن هناك رغبة بين عينة المستثمرين المصريين غير المحترفين في الاستثمار في أسهم هذه الشركة ، وبالنظر إلي جدول رقم (5) ، (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب كانت أكبر في حالة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني والذي يساوي (47.61)، بالمقارنة متوسط الرتب في حالة عدم الإفصاح، والذي يساوي (33.07)، وهو الأمر الذى يؤكد على إدراك المستثمرين غير المحترفين علي أهمية إفصاح الإدارة عن تقرير مخاطر الأمن السيبراني عند اتخاذهم لقرارات الاستثمار.

Wilcoxon Signed Ranks Test

جدول 5: Ranks

		N	Mean Rank	Sum of Ranks
SybrS - NonSybrS	Negative Ranks	7[a]	33.07	231.50
	Positive Ranks	85[b]	47.61	4046.50
	Ties	16[c]		
	Total	108		

a. SybrS < NonSybrS

b. SybrS > NonSybrS

c. SybrS = NonSybrS

جدول 6: Test Statistics[a]

	SybrS - NonSybrS
Z	-7.466-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on negative ranks.

ويري الباحث أن إتجاه الشركات المصرية للإفصاح عن إدارة مخاطر الأمن السيبراني، من شأنه أن يعطي معلومات تكون بمثابة دلالات وإشارات قوية للمستثمرين الأفراد غير المحترفين، تزيد من رغبتهم، وتمكنهم بحرية من إتخاذ قراراتهم سواء بقبول الاستثمار في حالة عدم تعرض الشركة لأحداث انتهاك سيبرانية، أو بالرفض في حالة حدوث اختراقات السيبرانية. وهو ما يزيد من ثقة المستثمرين تجاه الشركة ، ومن اتخاذ قرارات استثمارية رشيدة.

6-5-7-2 نتيجة اختبار الفرض الثاني(H2)

استهدف الفرض الثاني (H2) اختبار ما إذا كان التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين يختلف باختلاف نوع جنس المستثمر. **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر.

وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف نوع جنس المستثمر.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف نوع جنس المستثمر.

ويظهر الجدول التالى نتيجة اختبار الفرض الثاني **(H2)**

Wilcoxon Signed Ranks Test

جدول7: Ranks

		N	Mean Rank	Sum of Ranks
FeSybs - MaSybs	Negative Ranks	59[a]	30.00	1770.00
	Positive Ranks	0[b]	.00	.00
	Ties	2[c]		
	Total	61		

a. FeSybs < MaSybs

b. FeSybs > MaSybs

c. FeSybs = MaSybs

جدول8: Test Statistics[a]

	FeSybs - MaSybs
Z	-6.863-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

ووفقاً لاختبار ويلكوكسون جدول رقم (8) كانت قيمة P–Value (0.000) أقل من (5%)، **وبالتالي يتم رفض فرض العدم وقبول الفرض البديل(H2)**. القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر.

وتتفق هذه النتيجة مع ما توصل إليه كل من (Hira & Loibl, 2008; Mishra & Metilda, 2015; Jain & Mandot, 2012; Anwar et al., 2017; Fatokun et al., 2019). والتي تري أن العوامل مثل جنس المستثمر تؤثر علي سلوك ومعرفة وكفاءة ومعتقدات وتصورات المستثمرين الأفراد غير المحترفين بشأن الأمن السيبراني.

وبالنظر إلي جدول رقم (7) (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب في حالة جنس المستثمر الذكر والذي يساوي (30.0) ، أكبر من متوسط الرتب في حالة جنس المستثمر الانثي والذي يساوي (0.00). وهو ما يتفق مع كل من دراسة (Wood & Zaichkowsky, 2004; Mishra & Metilda, 2015) في أن المستثمرات النساء أكثر تحفظًا من الرجال عند اتخاذهم لقرار الاستثمار، بينما المستثمرون الرجال لديهم مستوى ثقة أعلى وتحمل للمخاطر عند اتخاذ قرارا الاستثمار. **ويري الباحث** أنه من الطبيعي أن يختلف المستثمرون الأفراد غير المحترفون في قراراتهم وفقاً لجنسهم والذي يؤثر علي معتقداتهم وتصوراتهم ورغبتهم.

6-5-7-3 نتيجة اختبار الفرض الثالث (H3)

استهدف الفرض الثالث(H3) اختبار ما إذا كان التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين يختلف باختلاف عمر المستثمر. **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين باختلاف العمر.

وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف عمر المستثمر.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف عمر المستثمر.

ويظهر الجدول التالى نتيجة اختبار الفرض الثالث (H3):

Wilcoxon Signed Ranks Test

جدول9: Ranks

		N	Mean Rank	Sum of Ranks
Smage - bigage	Negative Ranks	47[a]	24.00	1128.00
	Positive Ranks	0[b]	.00	.00
	Ties	0[c]		
	Total	47		

a. Smage < bigage

b. Smage > bigage

c. Smage = bigage

جدول10: Test Statistics[a]

	Smage - bigage
Z	-6.154-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

ووفقاً لاختبار ويلكوكسون جدول رقم (10) كانت قيمة P–Value (0.000) أقل من (5%)، وبالتالي **يتم رفض فرض العدم وقبول الفرض البديل(H3)**. القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف عمر المستثمر.

وتتفق هذه النتيجة مع بعض الدراسات (Lutfi, 2011; Menkhoff et al., 2013; Whitty et al., 2015) والتي تري أن عمر المستثمر يؤثر علي مستوى ثقته وقراراته الاستثمارية، وقدرته علي مواجهة التهديدات السيبرانية.

وبالنظر إلي جدول رقم (9) (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب في حالة عمر المستثمر الأكثر عمراً والذي يساوي (24.0)، أكبر من متوسط الرتب في حالة المستثمر الأقل عمراً والذي يساوي (0.00). وهو ما يتفق مع كل من دراسة (Chakraborty et al., 2016).

ويري الباحث أن عمر المستثمر، يمثل مؤشراً هاماً يؤثر علي سلوك المستثمرين الأفراد، من خلال تأثيرهم علي خبرتهم ومستوي تقبلهم للمخاطر، وتصوراتهم ومعتقداتهم، وبالتالي علي قراراته بشأن المعلومات عن مخاطر الامن السيبراني.

6-5-7-4 نتيجة اختبار الفرض الرابع (H4)

استهدف الفرض الفرعي(H4) اختبار ما إذا كان التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين يختلف باختلاف مستوي التأهيل العلمي للمستثمر. **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر.

وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف مستوي التأهيل العلمي للمستثمر.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف مستوي التأهيل العلمي للمستثمر.

ويُظهر الجدول التالى نتيجة اختبار الفرض الرابع (H4):

Wilcoxon Signed Ranks Test

جدول11: Ranks

		N	Mean Rank	Sum of Ranks
Nonqul - Qul	Negative Ranks	54[a]	27.50	1485.00
	Positive Ranks	0[b]	.00	.00
	Ties	0[c]		
	Total	54		

a. Nonqul < Qul

b. Nonqul > Qul

c. Nonqul = Qul

جدول 12: Test Statistics[a]

	Nonqul - Qul
Z	-6.602-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

ووفقاً لاختبار ويلكوكسون جدول رقم (12) كانت قيمة P–Value (0.000) أقل من (5%)، وبالتالي **يتم رفض فرض العدم وقبول الفرض البديل(H4)**. القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر.

وتتفق هذه النتيجة مع بعض (Schooley & Worden, 1999; Bhandari & Deaves, 2006; Lutfi, 2010; Obamuyi, 2013; Miazee & Hasan, 2014) والتي تري أن المستثمرون الذين لديهم مستوي تأهيل علمي لديهم المعرفة والمهارات التي تمكنهم باتخاذ قرارات الاستثمار، بشكل أفضل في التعامل مع التهديدات السيبرانية أكثر من غيرهم من الأقل تأهيلاً.

وبالنظر إلي جدول رقم (11) (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب في حالة المستثمر المؤهل علمياً والذي يساوي (27.5)، أكبر من متوسط الرتب في حالة المستثمر غير المؤهل والذي يساوي (0.00).

ويري الباحث أن ارتفاع مستوي تعليم المستثمر يحسن من قدراته ويمكنه من دراسته وفهمه للمعلومات المتعلقة بالفرص الاستثمارية، وتعاملة مع المخاطر والتهديدات السيبرانية.

6-5-7-5 نتيجة اختبار الفرض الخامس(H5)

استهدف الفرض الخامس(**H5**) اختبار ما إذا كان التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين يختلف باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي المستثمر معاً. **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي للمستثمر معاً. وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي للمستثمر معاً.

$H1$: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي للمستثمر معاً.

ويظهر الجدول التالى نتيجة اختبار الفرض الخامس (H5):

Wilcoxon Signed Ranks Test

جدول13: Ranks

		N	Mean Rank	Sum of Ranks
B - A	Negative Ranks	55[a]	28.00	1540.00
	Positive Ranks	0[b]	.00	.00
	Ties	0[c]		
	Total	55		

a. B < A

b. B > A

c. B = A

جدول14: Test Statistics[a]

	B - A
Z	-6.470-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

ووفقاً لاختبار ويلكوكسون جدول رقم (14) كانت قيمة P–Value (0.000) أقل من (5%)، وبالتالي **يتم رفض فرض العدم وقبول الفرض البديل(H5)**. القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي للمستثمر معاً.

وتتفق هذه النتيجة مع بعض ما أوضحته دراسات (Mohebzada, et al., 2012; Jain& Mandot, 2012; Geetha & Ramesh, 2012; Obamuyi, 2013; Mishra & Metilda, 2015; Lan et al., 2018). والتي تري أن بعض العوامل مثل؛ الجنس، والعمر، ومستوي العلمي والمعرفة تؤثر علي سلوك المستثمرين بشأن تقبلهم للمخاطر وتفضيلاتهم الاستثمارية وثقتهم وجودة قراراتهم، وتصوراتهم ومعتقداتهم بشأن مخاطر الأمن السيبراني.

وبالنظر إلي جدول رقم (13) (Mean Ranks) بالمخرجات الإحصائية، يتضح أن متوسط الرتب في حالة المستثمر الذكر والأكبر سناً والمؤهل علمياً والذي يساوي (28)، أكبر من متوسط الرتب في حالة غيره من المستثمرين والذي يساوي (0.00).

ويري الباحث أن كل من العمر والجنس والمستوى التعليمي تمثل عوامل مؤثرة علي المستثمرين الأفراد غير المحترفين بشأن تعاملهم مع المعلومات المتعلقة بالأمن السيبراني.

6-5-8 التحليلات الأخري

قام الباحث بإعادة اختبار العلاقة الرئسية محل الدراسة، في ظل تغيير طرق قياس المتغير التابع، وتغيير طبيعة العينة (تقسيم العينة)، وذلك بغرض توفير المزيد من الوضوح علي العلاقات الرئيسية بالتحليل الأساسي وذلك قياساً علي، عطية (2021)، وذلك كما يلي:

6-5-8-1 حالة تغيير طريقة القياس

يقوم الباحث في هذه الجزئية بتغير طريقة قياس المتغير التابع وهو؛ رغبة وقرار المستثمرين غير المحترفين بالاستثمار في أسهم هذه الشركة من عدمها، حيث يتم إعادة اختبار العلاقة الرئيسية محل الدراسة، من خلال التحول من المقياس المتعلق بتخصيص القيمة (صفر) للإجابة "**لا أرغب بالمرة**" إلي القيمة (عشرة) للإجابة "**أرغب تماما**"، إلي استخدام مقياس من درجتين، يأخذ القيمة(1) في حالة أن ردود العينة بالرغبة في الاستثمار في أسهم الشركة كانت أعلي من متوسط الدرجات(5)، ويأخذ القيمة(صفر) في حالة ردود العينة بالرغبة في الاستثمار في أسهم الشركة كانت أقل من أو يساوي متوسط الدرجات (5)، وذلك لتحديد مدي رغبتهم في الاستثمار في أسهم هذه الشركة، في حالة الإفصاح عن تقرير مخاطر الأمن السيبراني، مقابل عدم الإفصاح، وذلك قياساً علي (علي وصالح، 2021)، وكانت نتيجة اختبار الفرض الرئيسي للبحث في هذه الحالة، كما يلي:

Wilcoxon Signed Ranks Test

جدول15: Ranks

		N	Mean Rank	Sum of Ranks
B1 - A1	Negative Ranks	2[a]	22.00	44.00
	Positive Ranks	41[b]	22.00	902.00
	Ties	65[c]		
	Total	108		

a. B1 < A1

b. B1 > A1

c. B1 = A1

جدول16: Test Statistics[a]

	B1 - A1
Z	-5.947-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on negative ranks.

يتضح من الجدول السابق رقم (16) أن قيمة P–Value (0.000) أقل من (5%)، **وبالتالي يتم رفض فرض العدم وقبول الفرض البديل(H1). القائل بوجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. ومن ثم يتسق ذلك ما تم توصل إليه الباحث بالتحليل الأساسي ويؤكد صحته.**

6-5-8-2 حالة تغيير طبيعة العينة

قام الباحث بتقسيم العينة الإجمالية للدراسة إلى عينتين وهي؛ عينة أعضاء هيئة التدريس بالجامعات المصرية المختلفة. وعينة طلاب الدراسات العليا متمثلة في (الدبلوم والماجستير والدكتوراه)، وذلك قياساً علي، عطية (2021) ، واعتماداً على العلاقات الرئيسية بالتحليل الأساسي كما هو، بدون أى تعديلات، وقام الباحث بإعادة اختبار فرض البحث الأول في ظل تقسيم عينة الدراسة إلى العينتين الفرعيتين، كما يلي:

6-5-8-2-1 حالة عينة أعضاء هيئة التدريس (فقط)

لاختبار ما إذا كان إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني يؤثر معنوياً علي قرارات المستثمرين المصريين غير المحترفين. استخدم الباحث اختبار ويلكوكسون لعينتين غير مستقلتين، من أجل اختبار هذا الفرض، **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يؤثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين. وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

ويظهر الجدول التالى نتيجة اختبار الفرض الأول(H1) لعينة أعضاء هيئة التدريس :

Wilcoxon Signed Ranks Test

جدول17: Ranks

		N	Mean Rank	Sum of Ranks
WiSybs2 - NonSybs2	Negative Ranks	2[a]	10.25	20.50
	Positive Ranks	33[b]	18.47	609.50
	Ties	19[c]		
	Total	54		

a. WiSybs2 < NonSybs2

b. WiSybs2 > NonSybs2

c. WiSybs2 = NonSybs2

جدول18: Test Statistics[a]

	WiSybs2 - NonSybs2
Z	-4.884-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test

b. Based on negative ranks.

يتضح من الجدول السابق رقم (18) أن قيمة P–Value (0.000) أقل من (5%)، **وبالتالي يتم رفض فرض العدم وقبول الفرض البديل(H1). القائل** بوجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. ومن ثم يؤكد صحة ما تم توصل إليه الباحث بالتحليل الأساسي.

6-5-8-2-2 حالة عينة طلاب الدراسات العليا (فقط)

لاختبار ما إذا كان إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني يؤثر معنوياً علي قرارات المستثمرين المصريين غير المحترفين. واستخدم الباحث اختبار ويلكوكسون لعينتين غير مستقلتين، من أجل اختبار هذا الفرض، **وقد تم إعادة صياغته كفرض عدم كما يلى:**

H_0: لا يؤثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين. وتم صياغته كفرض إحصائي كما يلي:

H_0: Median (1) = Median (2)

H_0: لا يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

H1: Median (1) ≠ Median (2)

H_1: يختلف الوسيط في حالة إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني عن الوسيط في حالة عدم الإفصاح.

Wilcoxon Signed Ranks Test

جدول19: Ranks

		N	Mean Rank	Sum of Ranks
WiSybs4 - NonSybs4	Negative Ranks	31[a]	21.00	651.00
	Positive Ranks	5[b]	3.00	15.00
	Ties	2[c]		
	Total	38		

a. WiSybs4 < NonSybs4
b. WiSybs4 > NonSybs4
c. WiSybs4 = NonSybs4

جدول20: Test Statistics[a]

	WiSybs4 - NonSybs4
Z	-5.005-[b]
Asymp. Sig. (2-tailed)	.000

a. Wilcoxon Signed Ranks Test
b. Based on positive ranks.

يتضح من الجدول السابق رقم (20) أن قيمة P–Value (0.000) أقل من (5%)، **وبالتالي يتم رفض فرض العدم وقبول الفرض البديل(H1). القائل** بوجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. ومن ثم يؤكد صحة ما تم توصل إليه الباحث بالتحليل الأساسي.

6-5-9 خلاصة نتائج اختبار فروض البحث

يوضح الجدول التالي خلاصة نتيجة اختبار فروض البحث:

الفرض	صيغة الفرض	نتيجة اختبار الفرض في حالة التحليل الأساسي	نتيجة اختبار الفرض في حالة التحليلات الأخرى (تغيير طريقة القياس وطبيعة العينة)
الفرض الأول H1	يؤثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرارات المستثمرين المصريين غير المحترفين.	تم قبوله	تم قبوله
الفرض الثاني H2	يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر.	تم قبوله	
الفرض الثالث H3	يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف العمر.	تم قبوله	
الفرض الرابع H4	يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر.	تم قبوله	
الفرض الخامس H5	يختلف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف كل من نوع جنس وعمر ومستوي التأهيل العلمي للمستثمر معاً.	تم قبوله	

6-6- نتائج البحث والتوصيات ومجالات البحث المقترحة

يتناول هذا الجزء من البحث عرضاً لنتائج البحث، والتوصيات، ومجالات البحث المقترحة، وذلك علي النحو التالي:

6-6-1 نتائج البحث

تناول البحث دراسة واختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، **وقد خلص البحث إلي قبول الفرض (H1)** القائل بوجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين. ويتفق ذلك مع ما توصل إليه البحث في شقه النظري. وقد ترجع هذه النتيجة إلي أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، يوفر معلومات حول المخاطر السيبرانية التي تواجهها الشركة وكيفية إدارتها، مما يزيد من وعي المستثمرين، وتكون بمثابة دلالات وإشارات قوية لهم، تمكنهم من اتخاذ القرارات الاستثمارية الرشيدة سواء بالقبول في حالة عدم تعرض الشركة لأحداث انتهاك سيبرانية، أو بالرفض في حالة حدوث اختراقات السيبرانية. وهو ما يزيد من ثقتهم تجاه الشركة.

كما خلص البحث إلي قبول الفرض (H2) القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف نوع جنس المستثمر. ويتفق ذلك مع ما توصل إليه البحث في شقه النظري. وقد ترجع هذه النتيجة إلي أن نوع جنس المستثمر يؤثر علي سلوكه ومعرفته وكفاءته ومعتقداته وتصوراته بشأن الأمن السيبراني.

وأيضاً خلص البحث إلي قبول الفرض (H3) القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف عمر المستثمر. ويتفق مع ما توصل إليه البحث في شقه النظري. وقد ترجع هذه النتيجة إلي أن عمر المستثمر، يمكن يؤثر علي خبرته ومستوي تقبله للمخاطر، وتصوراته ومعتقداته، وبالتالي علي قراراته بشأن مخاطر الامن السيبراني.

كما خلص البحث إلي قبول الفرض (H4) القائل باختلاف التأثير المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين باختلاف مستوي التأهيل العلمي للمستثمر. ويتفق مع ما توصل إليه البحث في شقه النظري. وقد ترجع هذه النتيجة إلي أن ارتفاع مستوي تعليم المستثمر، ومستوي تأهيله العلمي، يوفر له المعرفة والمهارات التي تحسن من قدراته وتمكنه من دراسة وفهم المعلومات المتعلقة بالفرص الاستثمارية، بشكل أفضل، والتعامل مع التهديدات السيبرانية أكثر من غيره من الأقل تأهيلاً. **كما خلص البحث إلي قبول الفرض (H5)** القائل باختلاف التأثير

المعنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين غير المحترفين باختلاف كل من نوع جنس، وعمر، ومستوي التأهيل العلمي للمستثمر معاً. ويتفق مع ما توصل إليه البحث في شقه النظري. وقد ترجع هذه النتيجة إلي أن هذه العوامل من الممكن أن تؤثر علي كفاءته وسلوكياته ومعرفته ومهاراته، ومستوي فهمه وتفضيلاته، ومدي تقبله المخاطر، وتعامله التهديدات السيبرانية، ومستوى ثقته وجودة أحكامه عند اتخاذه للقرارات.

6-6-2 توصيات البحث

وفقاً لما انتهي إليه البحث من نتائج بشقيه النظري والتجريبي، وفي ضوء حدوده، يوصي الباحث بما يلي:

- ضرورة قيام هيئة الرقابة المالية بتقديم الدعم المستمر للشركات لحثها علي الإفصاح عن إدارتها لمخاطر الأمن السيبراني.
- من المهم أن تنشأ كل شركة لديها إدارة (أو قسم) خاصة بإدارة مخاطر الأمن السيبراني، وتقوم بتحديثها باستمرار، والتدريب المستمر لفريق العمل المعني بالأمن السيبراني، لثقل وتطوير مهاراتهم وتوعيتهم بخطورة الأحداث السيبرانية وعواقبها.
- ضرورة التواصل الفعال مع شركاء الأعمال وأصحاب المصالح لتطوير عملية الإفصاح وتحسين ممارسات الأمن السيبراني .
- يجب على الهيئة العامة للرقابة المالية وصانعي السياسات النظر فيما إذا كان ينبغي حث الشركات علي المزيد من الإفصاحات المتعلقة بالأمن السيبراني. وفرض عقوبات علنية وصارمة على الشركات لعدم التزامها بالإفصاح عن تعرضها للانتهاك السيراني ، وإتخاذ إجراءات تنظيمية لتعزيز الإفصاح في الوقت المناسب عن الانتهاكات السيبرانية.
- يجب أن تركز مقررات المحاسبة والمراجعة في مرحلة الدراسات العليا وكذا مؤتمرات أقسام المحاسبة المتخصصة بالجامعات المصرية علي قضية مخاطر الأمن السيبراني وإدارة هذه المخاطر.

6-6-3 مجالات البحث المقترحة

يقترح الباحث عدداً من مجالات البحوث المستقبلية، علي النحو التالي:

- أثر الإفصاح الإختياري للشركات عن إدارة مخاطر الأمن السيبراني علي قيمتها السوقية .
- أثر التوكيد المهني علي تقارير إدارة مخاطر الأمن السيبراني علي قرارات مانحي الائتمان.

- نحو تفسير منطقي لتباين مستوي إفصاح الشركات المقيدة بالبورصة المصرية عن إدارة مخاطر الأمن السيبراني.
- أثر اتجاه الشركات للاستثمار في الأمن السيبراني علي قرارات أصحاب المصالح.
- أثر خصائص مجلس الإدارة علي اتجاه الشركات للاستثمار في الأمن السيبراني.
- نحو تفعيل دور المراجعة الداخلية في تعزيز الإفصاح عن مخاطر الأمن السيبراني.
- أثر تنوع الجنس في مجلس الإدارة علي إتجاه الشركات للإفصاح عن تقرير إدارة مخاطر الامن السيبراني.
- أثر درجة الالتزام الحوكمي للشركة علي اتجاهها للإفصاح عن تقرير إدارة مخاطر الامن السيبراني.
- نحو تفسير منطقي لإختلاف جودة والمحتوي المعلوماتي لإفصاح الشركات عن إدارة مخاطر الأمن السيبراني في ضوء مدخل الأهمية النسبية .
- نحو تفسير منطقي لاختلاف قرارات المستثمرين غير المحترفين بشأن إفصاح الشركات عن إدارة مخاطر الأمن السيبراني في ضوء طبيعة الصناعة، والعوامل المؤسسية.
- أثر توقيت والمحتوي المعلوماتي لإفصاح الشركات عن حوادث الأمن السيبراني علي سلوك المستثمرين.
- أثر إفصاح الشركات المقيدة بالبورصة المصرية عن إدارة مخاطر الأمن السيبراني عبر وسائل التواصل الاجتماعي علي قرار الاستثمار في أسهمها– دراسة تجريبية.

المراجع

أولاً: المراجع باللغة العربية

الرشيدي، طارق عبد العظيم، السيد، داليا عادل، 2019، أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية علي أسعار الأسهم وأحجام التداول- دراسة مقارنة في قطاع تكنولوجيا المعلومات، ***مجلة المحاسبة والمراجعة***، كلية التجارة، جامعة بني سويف، العدد الثاني، ص 439-487.

الدليل التنظيمي للأمن السيبراني،2020، هيئة الاتصالات وتقنية المعلومات، السعودية، ص1-54 . متاح على: www.fra.gov.eg.

الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، 2019، هيئة سوق المالي السعودي.

الهيئة الوطنية للأمن السيبراني،2018، الضوابط الأساسية للأمن السيبراني، السعودية.

الإستراتيجية الوطنية للأمن السيبراني،2017، المجلس الأعلي للأمن السيبراني، رئاسة مجلس الوزراء جمهورية مصر العربية.

بدوي، هبه الله عبد السلام، 2021، أثر جودة ومستوي التوكيد علي برنامج إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين- دراسة تجريبية ، ***مجلة الإسكندرية للبحوث المحاسبية***، كلية التجارة، جامعة الإسكندرية، المجلد الخامس،العدد الثالث، ص 1-56.

عزام، عبد المرضي حامد، ويحي سعد زغلول، 2006، **الاستدلال الإحصائي: مدخل الي اتخاذ القرار والتنبؤ، قسم الإحصاء والرياضة والتأمين**، كلية التجارة، جامعة الإسكندرية.

عطية، سارة حمدي عبد الرسول، 2021، **أثر تبني معايير التقرير المالى الدولية على جودة المعلومات المحاسبية وقياس التصنيف الائتمانى للشركات، دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية**، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة دمنهور.

علي، محمود أحمد، وصالح علي صالح، 2021، أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار بالأسهم- دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، كلية التجارة، جامعة الإسكندرية، المجلد السادس، العدد الثالث، ص1-48.

ثانياً: المراجع باللغة الأجنبية

Abdullah M, Abdul S Z, Mohamed Z M & Ahmad A. (2015). Risk management disclosure: A study on the effect of voluntary risk management disclosure toward firm value. *Journal of Applied Accounting Research, 16* (3), 400-32.

Abdullah, M. D. F. (2019, November). The Effect of Corporate Risk Disclosure toward Firm Value in Indonesia Sharia Stock Index. In *IOP Conference Series: Materials Science and Engineering*, *662* (3), 032070.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4* (1), 1-15.

Ali, S. E. A., Lai, F.W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., & Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. *Computers & Security*, *110*,102451,www.sciencedirect.com.

American Institute of Certified Public Accountants (AICPA) (2017). Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program, AICPA Assurance Services Executive Committee, New York, NY.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23* (3), 1177-1206.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Aqel, S. (2011). Auditors' Assessments of Materiality Between Professional Judgment and Subjectivity. *Acta Universitatis Danubius. Œconomica*, *7* (4), 72-88.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312, w w w. e l s e v i e r .c o m.

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*, *41* (6), 1-23.

Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33* (10-11), 706-719.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37* (6), 508-526.

Bhandari, G., & Deaves, R. (2006). The demographics of overconfidence. *The Journal of Behavioral Finance*, *7* (1), 5-11.

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.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50* (4), 651-661.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47-56.

Chartered Professional Accountants (CPA) Canada. (2017). Cyber security risks and incidents: Reassessing your disclosure practices,www.cpacanada.ca.

Chen, J., Henry, E., & Jiang, X. (2022). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, 1-26, www.doi.org.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed?. *Journal of Information Systems*, *33* (3), 163-182.

Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. *Communications of the Association for Information Systems*, *50* (1), 26.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of information Systems*, *35* (2), 179-194.

Cole, C., Brendan Quigley, Clint Rancher & Robert Cowan. (2022). SEC Proposes Rules Mandating Disclosure of Material Cybersecurity Incidents, *The Corporate Governance Advisor 39* (6), *3-7.*

Committee of Sponsoring Organizations of the Treadway Commission(COSO). (2015). Governance and internal control,www.Coso.org.

Committee of Sponsoring Organizations of the Treadway Commission(COSO). (2020). Governance and Enterprise Risk Management ,www.Coso.org.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4* (10),13-23.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-39.

D'Arcy, J., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, *23* (3), 779-805.

Deaves, R., Luders, E., & Schroder, M. (2010). The dynamics of overconfidence: evidence from stock market forecasters. *Journal of Economic Behavior and Organization*, *75* (3), 402–412.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13* (2), C1-C9.

Farkas, M., & Murthy, U. S. (2014). Nonprofessional investors' perceptions of the incremental value of continuous auditing and continuous controls monitoring: An experimental investigation. *International Journal of Accounting Information Systems*, *15* (2), 102-121.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In *Journal of Physics: Conference Series*, 1339 (1), 012098.

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.

Galligan, M. E., & Rau, K. (2015). COSO in the cyber age. *Deloitte Global*,Research Commissioned by COSO, www.Coso.org.

Galligan, m. E., herrygers, s., & rau, k. (2020). Cyber risk in a digital age, Research Commissioned by COSO, www.Coso.org.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468, www .ScienceDirect.com.

Geetha, N., & Ramesh, M. (2012), A Study on Relevance of Demographic Factors in Investment Decisions. *International Journal of Financial Management* (IJFM), 1(1), 39-56.

Goel, S., & Shawky, H. A. (2014). The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems*, *34* (1), 3.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS quarterly*, 567-594.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security*, *73*, 345-358.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34* (7), 808-834.

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* ,www.semanticscholar.org.

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19* (2), 73-100.

Hilary , G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: who cares?. *Georgetown McDonough School of Business Research Paper*, (2852519),www.ssrn.com.

Hira, T. K., & Loibl, C. (2008). Gender differences in investment behavior. In *Handbook of consumer finance research* (pp. 253-270). Springer, New York, NY.

Iatridis, G. (2008). Accounting disclosure and firms' financial attributes: Evidence from the UK stock market. *International review of financial analysis*, *17*(2), 219-241.

International Auditing and Assurance Standards Board (IAASB). 2015.**The Auditor's Responsibilities Relating to Other Information**. International Standard on Auditing (ISA) 720 revised. New York, NY: IAASB Available at: www.ifac.org.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, *33* (4), 377-409.

Jain, D., & Mandot, N. (2012). Impact of Demographic Factors on Investment Decision of Investors in Rajasthan. *Journal of Arts, Science & Commerce*, 3(2), 81 -92.

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. *Journal of Information Systems*, *33* (3), A1-A2.

Jeske, D., & Van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, *66*, 129-141.

Jin, J. (2015). Cybersecurity disclosure effectiveness on public companies, www, googel.com.

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33* (4), 360-376.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139* (3), 719-749.

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, www.nber.org.

Kelton, A. S. (2021). How to Reduce the Cybersecurity Breach Contagion Effect. *Current Issues in Auditing*, *15* (2), 1-9.

Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. *Journal of Information Systems*, *34* (3), 133-157.

Khalil, A., & Maghraby, M. (2017). The determinants of internet risk disclosure: empirical study of Egyptian listed companies. *Managerial Auditing Journal*, *32*(8), 746-767.

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27* (1), 219-236.

Lan, Q., Xiong, Q., He, L., & Ma, C. (2018). Individual investment decision behaviors based on demographic characteristics: Case from China. *PloS one*, *13* (8), e0201916.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40-55.

Lutfi, L. (2011). The relationship between demographic factors and investment decision in Surabaya. *Journal of Economics, Business, & Accountancy Ventura*, *13* (3), 213-224.

Mahastanti, L. A. (2011). Faktor-faktor yang dipertimbangkan investor dalam melakukan investasi. *Jurnal Manajemen Teori dan Terapan*, *4*(3), 37-51.

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, *76* (2), 131-140.

Menkhoff, L., Schmeling, M., & Schmidt, U. (2013). Overconfidence, experience and professionalism: an experimental study. Journal of Economic Behavior and Organization, 86(C), 92–101.3. Elsevier.

Miazee, M. H., Shareef, A. N. M., & Hasan, M. N. (2014). Fundamentals knowledge of investor and its influence on investment in capital market-A study from Dhaka stock exchange. *Research Journal of Finance and Accounting*, 5(24), 7-19.

Mishra, K. C., & Metilda, M. J. (2015). A study on the impact of investment experience, gender, and level of education on overconfidence and self-attribution bias. *IIMB Management Review*, *27* (4), 228-239.

Mohebzada, J. G., El Zarka, A., BHojani, A. H., & Darwish, A. (2012, March). Phishing in a university community: Two large scale phishing experiments. In *2012 international conference on innovations in information technology (IIT)*, 249-254. IEEE.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2017). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *The Business Lawyer*, *73* (1), 1-34.

Mousa, G., & Elamir, E. (2013). Content analysis of corporate risk disclosures: the case of Bahraini capital market. *Global review of Accounting and Finance*, *4*(1), 27-54.

Mousa, G., & Elamir, E. (2013). Content analysis of corporate risk disclosures: the case of Bahraini capital market. *Global review of Accounting and Finance*, *4*(1), 27-54.

Nordlund, J. (2021). The disclosure of cybersecurity risk. *www. SSRN*.com

Obamuyi, T. M. (2013). Factors influencing investment decisions in capital market: A study of individual investors in Nigeria. *Organizations and markets in emerging economies*, *4*(1), 141-161.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Perols, R. R. (2019). Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions, www.digitalcommons.usf.edu.

Pompian, M. M., & Longo, J. (2004). A new paradigm for practical application of behavioural finance: creating investment programs based on personality types and gender to produce better investment outcomes. *The Journal of Wealth Management*, *7*(2), 9–15.

Public Company Accounting Oversight Board (PCAOB). 2018. Strategic plan2018–2022,www.pcaobus.org.

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of business ethics*, *177*(2), 351-374.

Ramírez, M., Rodríguez Ariza, L., & Gómez Miranda, M. E. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability*, *14*(3), 1-23.

Roskot, M., Wanasika, I., & Kroupova, Z. K. (2020). Cybercrime in Europe: surprising results of an expensive lapse. *Journal of Business Strategy, 42* (2), 91-98.

Schooley, D. K., & Worden, D. D. (1999). Investors' asset allocations versus life-cycle funds. *Financial Analysts Journal*, *55* (5), 37-43.

Securities and Exchange Commission(SEC). (2011). CF Disclosure Guidance: Topic No. 2 Cybersecurity. *Washington, DC: US Securities and Exchange Commission*, www.sec.gov.

Securities and Exchange Commission(SEC). (2018).. 17 CFR Parts 229 and 249. [Release Nos. 33-10459; 34-82746].Commission Statement and Guidance on Public Company Cybersecurity Disclosures, www.sec.gov.

Securities and Exchange Commission (SEC). (2022).Release No. 33-11038, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, www.sec.gov.

Shaikh, A. R. H., & Kalkundrikar, A. B. (2011). Impact of Demographic Factors on Retail Investors' Investment Decisions- An Exploratory Study. *Indian Journal of Finance,* 5(9), 35 – 44.

Shanmugsundaram,V., & Balakrishnan, V.(2011). Investment Decisions – In&uence of Behavioural Factors. Indian Journal of Finance, 5(9), 25 – 34.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216-229.

Sulistyaningsih, S., & Gunawan, B. (2018). Analisis faktor-faktor yang memengaruhi risk management disclosure (Studi empiris pada perusahaan manufaktur yang terdaftar di Bursa Efek Indonesia tahun 2012-2014). *Riset akuntansi dan keuangan Indonesia*, *1*(1), 1-11.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. *Journal of Forensic and Investigative Accounting*, *12* (2), 197-212.

Szubartowicz, E., & Schryen, G. (2020). Timing in information security: An event study on the impact of information security investment announcements. *Journal of Information System Security*, *16* (1).

Tayaksi, C., Ada, E., Kazancoglu, Y., & Sagnak, M. (2021). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. *Journal of Enterprise Information Management,35* (2), 650-668.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795, www. ScienceDirect.org.

Walton, S., Wheeler, P. R., Zhang, Y. I., & Zhao, X. R. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, *35* (1), 155-186.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

Wood, R., & Zaichkowsky, J. L. (2004). Attitudes and trading behavior of stock market investors: A segmentation approach. *The Journal of Behavioral Finance*, *5* (3), 170-179.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, 375-382.

Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, *,28* (1), 167-183.

ملحق (1)

الدراسة التجريبية

كلية التجارة– جامعة دمنهور

قسم المحاسبة

السيد الأستاذ الفاضل/ .....

تحية طيبة وبعد،،،،،،،،،

يقوم الباحث بإعداد بحث في مجال **الإفصاح عن إدارة مخاطر الأمن السيبراني من منظور أصحاب المصالح**. وتمثل الحالات المرفقة أحد أهم أدوات البحث لإجراء الدراسة التجريبية.

والباحث إذ يشكركم مسبقاً علي حسن تعاونكم معه ليرجو التكرم بقراءة الحالات التالية، **والإجابة علي كافة الاسئلة المرافقة لها بوضوح**، حيث يمثل ذلك جزء من متطلبات تحقيق الهدف من البحث.

وتفضلوا سيادتكم بقبول فائق الاحترام،،،،،،،

الباحث/ د. إبراهيم أحمد شرف

أستاذ المحاسبة والمراجعة المساعد

كلية التجارة – جامعة دمنهور

Ibrahim_shraf2000@yahoo.com

أولاً: البيانات الشخصية

- **الاسم:** ..... (اختياري).
- **النوع:** ذكر ( ) أنثي ( ).
- **العمر:** ( ).
- **الوظيفة الحالية:** .....
  - دراسات عليا ( ).
  - معيد ( ).
  - مدرس مساعد ( ).
  - مدرس ( ).
  - أستاذ مساعد ( ).
  - أستاذ ( ).
- **عضوية جمعيات مهنية** ( ).
- **شهادات مهنية إن وجدت** ( ).

ثانياً: المصطلحات الفنية ذات الصلة بموضوع البحث

1. **الأمن السيبراني Cybersecurity:** مجموعة التقنيات والعمليات والاجراءات المصممة لحماية الشبكات والأنظمة وأجهزة الكمبيوتر والبرامج وقواعد البيانات من الهجوم الالكتروني أو التلف أو الوصول غير المصرح به، أو التعطيل أو الاستغلال غير المشروع (AICPA 2017; Cheng et al.,2022).
2. **مخاطر الأمن السيبراني Cybersecurity Risks:** تشير إلى أي حدث يهدد أو يشكل تهديدًا لنظام المعلومات أو المعلومات التي يعالجها النظام أو يخزنها أو ينقلها(Frank et al., 2019)
3. **إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management:** تشير إلى عملية تنفيذ الشركة لمجموعة من السياسات والعمليات والاجراءات الرقابية والضوابط المصممة لحماية معلوماتها وأنظمتها الالكترونية من الأحداث والتهديدات السيبرانية التي يمكن أن تعوق تحقيق أهداف الشركة(AICPA 2017).

ثالثاً: الحالات التجريبية

شركة "السلام" شركة مساهمة مصرية تعمل في مجال الاتصالات. خاضعة للقانون 159 لسنة 1981 ومقيدة بالبورصة. تقوم بإعداد القوائم المالية وفقا لمعايير المحاسبة المصرية الصادرة لسنة 2015 وتعديلاتها. وقد بدأت الشركة عملياتها منذ أكثر من 30 عامًا.

وفيما يلي القوائم المالية للشركة عن السنة المنتهية في 31 /2021/12.

1- قائمة المركز المالي المختصرة لشركة "السلام" في نهاية عام 2021 (بالالف جنيه)

بيان	2021/12/31	2020/12/31
إجمالي الأصول المتداولة (1)	13946183	15167033
إجمالي الأصول طويلة الأجل(ملموسة وغير الملموسة) (2)	67149983	59731167
إجمالي الأصول (1) + (2)	**81096166**	**74898200**
إجمالي حقوق الملكية (3)	34741602	30060624
إجمالي الالتزامات (4)	46354564	44837576
اجمالي حقوق الملكية و الالتزامات (3) + (4)	**81096166**	**74898200**

2- قائمة الدخل المختصرة لشركة"السلام" عن السنة المنتهية في 2021/12/31 (بالالف جنيه)

بيان	2021/12/31	2020/12/31
إيرادات النشاط	27787127	24595916
تكلفة النشاط	(18254022)	(16551054)
مجمل ربح النشاط	9533105	8044862
إيرادات التشغيل الأخري	666507	538546
مصروفات التشغيل	(5986866)	(5695617)
صافي ربح النشاط	4212746	2887791
إيرادات أخري	5234098	1355955
مصروفات أخري	(1233725)	(1503061)
صافي الدخل قبل الضريبة	8213119	2740685
إجمالي ضريبة الدخل	(1257188)	(581159)
صافي ربح العام	6955931	2159526
نصيب السهم من ربح العام	3,66	,87

3- قائمة الدخل الشامل عن السنة المنتهية في 2021/12/31 (بالالف جنيه)

بيان	2021/12/31	2020/12/31
صافي ربح العام	**6955931**	**2159526**
بنود الدخل الشامل الاخر	-	-
إجمالي الدخل الشامل	**6955931**	**2159526**

4- قائمة التدفقات النقدية المختصرة عن السنة المنتهية في 2021/12/31 (بالالف جنيه)

بيان	2021/12/31	2020/12/31
صافي التدفقات النقدية الناتجة من الأنشطة التشغيلية	17479023	9693588
صافي التدفقات النقدية الناتجة من الأنشطة الاستثمارية	(9037789)	(9035698)
صافي التدفقات النقدية الناتجة من الأنشطة التمويلية	(5207400)	3452964
صافي التغير في النقدية وما في حكمها خلال العام	736139	853013
النقدية وما في حكمها خلال العام	1538732	685719
النقدية وما في حكمها أخر العام	**2274871**	**1538732**

5- قائمة التغير في حقوق الملكية المختصرة عن السنة المنتهية في 2021/12/31 (بالالف جنيه)

بيان	2021/12/31	2020/12/31
راس المال المصدر والمدفوع	17070716	**17070716**
إحتياطيات	5011376	**4903361**
أرباح مرحلة	3756805	4831887
توزيعات أرباح	(1946774)	(1095134)
صافي ربح العام	6955931	2159526
إجمالي حقوق الملكية	**34741602**	**30060624**

6- الإيضاحات المتممة عن السنة المنتهية في2021/12/31

- **أسس إعداد القوائم المالية:** يتم إعداد القوائم المالية وفقاً لمعايير المحاسبة المصرية والدولية (فيما لم يصدر بشأنه معايير محاسبة مصرية)، والقوانين المصرية واللوائح ذات الصلة. **التقديرات المحاسبية والافتراضات الرئيسية:** يتم استخدام تقديرات معقولة كأساس لإعداد القوائم المالية الموحدة وفقاً لمعايير المحاسبة المصرية. وتعتمد تقديرات الإدارة علي خبراتها التاريخية وتقارير المتخصصيين من خارج الشركة إذا لزم الأمر، ويتم مراجعتها. **ويتم قياس الأصول الثابتة بالتكلفة التاريخية.** وتتضمن الأصول

غير الملموسة مبلغ 10 مليون جنيه منصات رقمية وبرامج جاهزة مقومة بتكلفتها في تاريخ الاقتناء المساوية لقيمتها العادلة في ذلك التاريخ.

الحالة الأولى: تم نشر التقارير المالية للشركة معتمدة من مراقب الحسابات برأي نظيف في 2021/3/31 . في ضوء قراءتك للقوائم المالية السابقة وإيضاحاتها المتممة عن عام 2021، إذا علمت أن سعر إقفال سهم الشركة في 2020/12/31 ، 31 /2021/12 كان 13، 15 جنيه علي التوالي. وبإفتراض أنك مستثمر بالأسهم:

1- هل ترغب في الاستثمار في أسهم هذه الشركة؟

صفر لا أرغب بالمرة	1	2	3	4	5	6	7	8	9	10 أرغب تماما

2- هل تتوقع أن سعر اقفال أسهم الشركة في 2022/12/31 :

أ- يظل ثابتا عند 15 جنيه كما كان في 2021/12/31.

ب- يقل عن 15 جنيه.

ج- يزيد عن 15 جنيه.

الحالة الثانية: إفترض في الحالة السابقة ما يلي:

- أن الشركة لديها إدارة مخاطر بها قسم خاص بإدارة مخاطر الأمن السيبراني.
- أن مدير إدارة المخاطر اعتمد تقرير نائبه عن إدارة مخاطر الأمن السيبراني الذي ظهر **كالتالي:**

تقرير إدارة مخاطر الأمن السيبراني لشركة (السلام) لعام 2021

السادة / الهيئة العامة للرقابة المالية

إدارة البورصة المصرية

مجلس إدارة الشركة

قامت الشركة بتصميم ووضع إطار للتقرير عن إدارة مخاطر الأمن السيبراني التي تواجهها، وفقاً لمجموعة من الإصدارات المحاسبية والمهنية. ويتمثل برنامج إدارة مخاطر الأمن السيبراني للشركة في مجموعة من التقنيات والسياسات والعمليات والإجراءات الرقابية والضوابط المصممة لحماية معلوماتها وأنظمتها الإلكترونية من التلف أو الوصول غير المصرح به، أو التعطيل أو الاستغلال غير المشروع، وغيرها من الأحداث والتهديدات السيبرانية، والتي يمكن أن تعوق تحقيق الشركة لأهدافها. كما يلي:

- قام مجلس إدارة الشركة بإعداد إدارة خاصة للأمن السيبراني، وإنشاء فريق إدارة المخاطر الإلكترونية متعدد الوظائف، ويقوم بالاشراف عليها، وتدمج الشركة إدارة المخاطر السيبرانية في الخطة الإستراتيجية للشركة.
- تقوم الشركة بتحديد واضح لأهدافها المتعلقة بعملياتها وتقاريرها المالية وغير المالية، لتتمكن من إدارة المخاطر السيبرانية التي تواجهها، والتي تؤثر على تحقيقها لأهدافها، وإتخاذ القرارات بشأن الرقابة عليها.
- قامت الشركة بتصميم هيكل رقابة للامن السيبراني لمواجهة المخاطر وتقوم بعمل تقييم مستمر للتأكد من فاعلية تصميم وتشغيل الضوابط الداخلية، ومعالجة أوجه القصور واتخاذ الإجراءات التصحيحية.
- تقوم الشركة بمجموعة من الأنشطة والسياسات والاجراءات الرسمية للرقابة العامة على التكنولوجيا لضمان المخاطر السيبرانية عند مستوى مقبول.
- تقوم الشركة بتحديد وتحليل وتقييم المخاطر السيبرانية التي تواجهها، والنظر في احتمالية وقوعها من حيث حجم وكم ونوع تلك المخاطر، والتكاليف والعواقب المحتملة الناتجة عن تلك الحوادث، والتي تؤثر على تحقيق أهدافها؟.
- تقوم الشركة بتقييم المخاطر بطريقة شاملة، متضمنة مدى كفاية الإجراءات الوقائية المتخذة لتقليل مخاطر الأمن السيبراني وتأخذ في الاعتبار مخاطر الصناعة، والاعتبارات البيئية والتكنولوجية، والتغييرات التنظيمية والتغييرات الأخرى.
- تنشر الشركة أنشطة الرقابة، في شكل مجموعة من السياسات، والإجراءاتوالضوابط التي تمنع أو تكتشف الانتهاكات السيبرانية، في حالة حدوثها، وتقوم بالافصاح عنه، واتخاذ الإجراءات التصحيحية، كما تقوم بتطوير أنشطة الرقابة التي تساهم في التخفيف من المخاطر إلى مستويات مقبولة.

- تدعم الشركة هيكل الرقابة الداخلية بالمزيد من المعلومات الخارجية ذات الصلة التجارية والصناعية، وتقوم بمشاركة هذه المعلومات بين شركاء الأعمال والتحالفات الموثوقة، والتي يمكن أن تساعد في منع أو اكتشاف المخاطر السيبرانية .
- لدي الشركة قنوات للتواصل وتبادل المعلومات داخل الشركة بين جميع العاملين في كل المستويات، فيما يتعلق بأهداف ومسؤوليات الرقابة الداخلية ، لمساعدة الإدارة، والأفراد الذين يضطلعون بمسؤولياتهم المتعلقة بالرقابة الالكترونية.
- تتواصل الشركة مع الأطراف الخارجية من العملاء وشركاء الأعمال، والمنظمين، والمحللين الماليين، والجهات الحكومية، وأطراف خارجية أخرى بخصوص المخاطر السيبرانية، والتي تؤثر على تيسير عمل الرقابة الداخلية، و تسبب ضرر محتمل.
- تستعين الشركة بمتخصصين مؤهلين في مجال المخاطر الإلكترونية.
- يتم إجراء تقييم مستمر للتغييرات التي تطرأ والمتعلقة، بالأفراد، والعمليات، والتقنيات، والتي يمكن أن تؤثر على فاعلية هيكل الرقابة الداخلية، وعمل تحديث لتقييم المخاطر على أساس مستمر لتعكس التغييرات.
- تقوم الشركة بإجراء تقييم مستمر ودوري للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني، والضوابط للتأكيد على فعالية إدارة الأمن السيبراني، بهدف تقليل التعرض المحتمل للمخاطر السيبرانية.
- الإلتزام بالإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية وخاصة الحوادث الجوهرية وغير الجوهرية والتي تكون في المجمل جوهرية، في حالة حدوثها خلال السنة السابقة ، وأنواعها ومدي تكرارها.
- تقوم الشركة بوصف للتغطية التأمينية ذات الصلة بالحوادث السيبرانية، والتكاليف والعواقب الأخرى.
- تقوم الشركة بالتدريب المستمر للعاملين لتعزيز وعيهم بشأن الانتهاكات السيبرانية .
- تقوم الشركة بالافصاح الدوري عن الاستراتيجيات والسياسات والإجراءات المتبعة في حوكمة مخاطر الأمن السيبراني، وتحدد المسؤول عن حوكمة الأمن السيبراني.
- تلتزم الشركة بالتقرير عن النزاهة والأخلاق وفقا لمعايير السلوك بالشركة ، وتحديد ومعالجة الانحرافات، لدعم أداء برنامج إدارة مخاطر الأمن السيبراني.

التاريخ : 2021/3/31

التوقيع

عضو مجلس الإدارة المنتدب

- تتبني إدارة الشركة سياسة الإفصاح عن تقرير إدارة المخاطر بما فيها مخاطر الأمن السيبراني ضمن مرفقات القوائم المالية. ولذلك، تم ارسال هذا التقرير إلي هيئة الرقابة المالية وإدارة البورصة مرفقاً بالقوائم المالية لسنة 2021.
- **في ضوء قراءتك للقوائم المالية وتقرير إدارة مخاطر الأمن السيبراني وبصفتك مستثمر بأسهم الشركة إذا علمت أن سعر إقفال سهم الشركة في 2020/12/31،31 /2021/12 كان 13، 15 جنيه علي التوالي. وبإفتراض أنك مستثمر بالأسهم:**

1- هل ترغب في الاستثمار في أسهم هذه الشركة؟

صفر لا أرغب بالمرة	1	2	3	4	5	6	7	8	9	10 أرغب تماما

2- هل تتوقع أن سعر إقفال أسهم الشركة في 2022/12/31:

أ- يظل ثابتا عند 15 جنيه كما كان في 2021/12/31.

ب- يقل عن 15 جنيه.

ج- يزيد عن 15 جنيه.