أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الإستثمار في الشركات الصغيرة والمتوسطة الحجم

دراسة تجريبية علي الشركات المقيدة بالبورصة المصرية

د/ كريم محمد حافظ توفيق القاضي
مدرس المحاسبة والمراجعة بقسم نظم معلومات الأعمال
المعهد العالي للسياحة والفنادق والحاسب الآلي
السيوف – الإسكندرية
dr.karim.hafez.elkady@gmail.com

ملخص البحث

يهدف هذا البحث إلي دراسة وتحليل أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في الشركات الصغيرة والمتوسطة الحجم، ودراسة وتحليل المحتوي المعلوماتي لتقرير الإفصاح عن إدارة مخاطر الأمن السيبراني والقوانين والتشريعات الدولية المتعلقة بتطبيقه، كما يهدف ايضاً الي دراسة مفاهيم إدارة مخاطر الأمن السيبراني وأهميتها ومحددات الإفصاح عنها. وقدم الباحث منهجية نظرية ترتكز على قسمين رئيسين ترتبط بمتغيرات البحث وتحقق أهدافه، وكذلك إجراء دراسة تجريبية على عينة مكونة من 253 شركة من الشركات الصغيرة والمتوسطة الحجم التي تعمل بالسوق المصري، وقد تم استخدام مجموعة من الأساليب الإحصائية من خلال برنامج SPSS لتحليل البيانات واختبار الفروض.

وتوصل الباحث إلى العديد من النتائج أهمها: يؤثر تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم بالبيئة المصرية من حيث: دقة وموضوعية المعلومات المفصح عنها، زيادة مستوى الإفصاح والشفافية، والمساهمة في توفير معلومات كافية ودقيقة لتقييم الأداء. كما تبين وجود علاقة إيجابية معنوية بين تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم محل الدراسة باختلاف مستوي خبرة المستثمر. ويوجد ايضاً علاقة إيجابية معنوية بين تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم محل الدراسة باختلاف مستوي التأهيل العلمي للمستثمر. بينما لا يوجد علاقة ذات دلالة معنوية بين تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم محل الدراسة باختلاف مستوي التنمية المهنية المستثمر.

الكلمات المفتاحية: الأمن السيبراني – تقرير الإفصاح عن مخاطر الأمن السيبراني – قرار الاستثمار في الأسهم – خبرة المستثمر – التأهيل العلمي للمستثمر – التأهيل المهني للمستثمر.

[1] تقديم البحث في 2023/12/24 وقبول نشره في 2024/2/15

The Impact of Cybersecurity Risk Management Report Disclosure on Investment Decisions in Small and Medium-Sized Companies

An Empirical Study on Companies Listed on The Egyptian Stock Exchange

Abstract

The main objective of the research is to study and analyze the impact of the disclosure of the cybersecurity risk management report on investment decisions in small and medium-sized companies, and to study and analyze the informational content of the cybersecurity risk management disclosure report and international laws and legislation related to its application. It also aims to study the concepts of cybersecurity risk management. Its importance and determinants of disclosure. The researcher presented a theoretical methodology based on two main sections that relate to the research variables and achieve its objectives, as well as conducting an experimental study on a sample of 253 small and medium-sized companies operating in the Egyptian market. A set of statistical methods were used through the SPSS program to analyze the data and test the hypotheses.

The researcher reached many results, the most important of which are: The disclosure report on cybersecurity risk management affects investment decisions in shares of small and medium-sized companies in the Egyptian environment in terms of: accuracy and objectivity of the information disclosed, increasing the level of disclosure and transparency, and contributing to providing sufficient and accurate information to evaluate performance. It was also shown that there is a positive, significant relationship between the disclosure report on cybersecurity risk management and investment decisions in the shares of small and medium-sized companies under study, depending on the level of investor experience. There is also a significant positive relationship between the disclosure report on cybersecurity risk management and investment decisions in the shares of small and medium-sized companies under study depending on the level of educational qualification of the investor. While there is no significant relationship between the disclosure report on cybersecurity risk management and investment decisions in the shares of small and medium-sized companies under study, depending on the level of professional development of the investor.

Keywords: Cybersecurity - Cybersecurity risk disclosure report - Stock investment decision - Investor experience - Investor academic qualification - Investor professional qualification.

1. مقدمة

لا شك أن المؤسسات الصغيرة والمتوسطة تعتبر عنصراً أساسياً في نمو واستقرار الاقتصادات حول العالم. ونظرًا للدور الحيوي الذي تلعبه الشركات الصغيرة والمتوسطة في خلق فرص العمل، وضعت الحكومة المصرية على رأس أولوياتها تسهيل عمليات تمويل تلك الشركات وتنمية أعمالها. ففي عام 2016، قام البنك المركزي المصري بإطلاق مبادرة لتشجيع منح القروض متوسطة وطويلة الأجل للشركات الصغيرة والمتوسطة. كما ألزم البنوك بتخصيص 20٪ من إجمالي المحافظ الائتمانية لتمويل هذه الشركات بهدف منح ما يقرب من 200 مليار جنيه لتمويل 350 ألف شركة وخلق 4 ملايين فرصة عمل جديدة. ونتيجة لذلك، قامت البنوك المصرية بتقديم المزيد من القروض للشركات الصغيرة والمتوسطة، وبحلول عام 2019، ارتفعت قيمة تلك القروض إلى 146 مليار جنيه. واستنادا إلي بيانات البنك المركزي المصري فيبلغ عدد المنشآت المتناهية الصغر 3.4 مليون منشأة, والمتوسطة 2200 منشأة, والصغيرة 217 ألف منشأة. وقد قام البنك المركزي المصري بتصنيف الشركات الصغيرة والمتوسطة وفقًا لحجم أعمالها، ليتراوح ما بين مليون جنيه مصري و50 مليون جنيه مصري في الشركات الصغيرة، ويتراوح ما بين 50 مليون جنيه مصري و200 مليون جنيه مصري للشركات المتوسطة.

تقدم هذه الحقائق مثالاً على أهمية الشركات الصغيرة والمتوسطة الحجم لاستقرار ونمو الاقتصاد المصري. كما أصبحت تكنولوجيا المعلومات مطلبًا أساسيًا للشركات الصغيرة والمتوسطة الحجم بسبب الفوائد التي يمكن تحقيقها من خلال الاعتماد على هذه التقنيات. توفر تكنولوجيا المعلومات إمكانية وصول واسعة النطاق إلى العديد من الخدمات الأساسية مثل الشبكات عبر الإنترنت، والأهم من ذلك أنها تسمح بمشاركة البيانات والمعلومات بين موظفي الشركة. على سبيل المثال، تعد الحوسبة السحابية مثالًا رائعًا لتكنولوجيا المعلومات المفيدة في الوقت الحاضر. وتعاني ميزانيات المنظمات من الاضطرار إلى التعامل مع الظروف الاقتصادية الصعبة، في حين توفر تقنيات تكنولوجيا المعلومات مثل الحوسبة السحابية المزيد من الفرص لخفض التكاليف. ومثال آخر هو التجارة الإلكترونية، التي ظهرت كابتكار مهم في العقدين الأخيرين، وأصبحت شكلاً ضروريًا من أشكال التكنولوجيا في عالم الأعمال. علاوة على ذلك، اضطرت الشركات الصغيرة والمتوسطة، مثل غيرها من الشركات، إلى اعتماد التجارة الإلكترونية من أجل الازدهار في البيئة الاقتصادية التنافسية الحالية. يعد استخدام تكنولوجيا المعلومات الموثوقة في المؤسسات الصغيرة عاملاً رئيسياً يدعم نموها ويعزز ميزتها التنافسية. على الرغم من كل هذه الحقائق حول فوائد استخدام تكنولوجيا المعلومات للشركات الصغيرة والمتوسطة، يمكن لمجرمي الإنترنت استغلال بعض الجوانب السلبية. قد تكون تكنولوجيا المعلومات مثل الحوسبة السحابية هدفًا ذو أولوية عالية للمهاجمين السيبرانيين إذا تم بالفعل تحديد نقاط الضعف لدى مقدمي الخدمة.

في الآونة الأخيرة، أصبح الأمن السيبراني قضية رئيسية في مجال تكنولوجيا المعلومات، وذلك بسبب أهمية هذه الظاهرة في عدة مجالات مثل الأمن القومي والنظام التجاري العالمي. حيث أدي الاعتماد المتزايد من جانب معظم الشركات حول العالم علي تقنيات التخزين علي شبكات الإنترنت إلي زيادة احتمال تعرضها للهجمات السيبرانية، وهذا يجعل الأمن السيبراني مهماً جداً للشركات والمديرين وأعضاء مجلس الإدارة والمستثمرين وأصحاب المصالح المتنوعين (Frank et al.,2019). وقد تم تعريف الأمن السيبراني على أنه "مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم". ويعاني مديري الشركات المتوسطة والصغيرة الحجم من نقص المعرفة والوعي بأهمية الأدوات الأمنية، مما أثر على معدل اعتمادهم علي الأمن السيبراني.

ودعت بيئة الأعمال العالمية الشركات للحفاظ علي بنية تحتية رقمية صالحة وآمنة لإجراء معاملاتها التجارية، وتسمي البنية التحتية الرقمية المترابطة بالفضاء السيبراني[1] وتشمل الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والمعلومات الرقمية (الاستراتيجية الوطنية للأمن السيبراني, 2017). وقد تم تشجيع الشركات الصغيرة والمتوسطة الحجم على الاستفادة من أي فرص تجارية محتملة من خلال استخدام واعتماد تقنيات جديدة مثل خدمات الحوسبة السحابية. ولكن من ناحية أخري, هناك العديد من التهديدات المتعلقة بالأمن السيبراني, حيث أكد المديرين التنفيذيين لعدد من الشركات علي التأثير السلبي لقضايا الأمن السيبراني علي ثقة أصحاب المصلحة في الشركات وفي الصناعة (KPMG,2018; PWC,2019). حيث أن الهجوم الإلكتروني الذي يؤثر علي تلف أو فقد بعض المعلومات المالية للشركات يكون له تأثير سلبي علي أسعار الأسهم ومن ثم قرارات الاستثمار. ومع ذلك, هناك سوء فهم كبير للتهديدات السيبرانية من منظور الإدارة. حيث يؤدي التقليل من تهديدات الأمن السيبراني من قبل الشركات الصغيرة والمتوسطة إلى زيادة نقاط الضعف والمخاطر، والتي لسوء الحظ يمكن أن تصبح تحديات فعلية لها وللأطراف الأخرى ذات الصلة.

1- الفضاء السيبراني: الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد.

ولذلك, أصبحت إدارة المخاطر في الوقت الحاضر هذه مسألة خطيرة تؤثر عادة على أداء الشركات الصغيرة والمتوسطة الحجم لأسباب مختلفة مثل نقص الموارد ونقص الآليات التي يمكن أن تدعم نشاط إدارة المخاطر بشكل عام. علاوة على ذلك، تواجه الشركات الصغيرة والمتوسطة الحجم دائما، مثل الشركات الكبيرة، مخاطر مختلفة؛ والأهم من ذلك، أن وجودهم أكثر عرضة للخطر في أي وقت بسبب صغر حجم مواردهم المالية وغير المالية على حد سواء. عادة، تُظهر استراتيجيات الأعمال اهتمامًا أقل بآثار إدارة المخاطر، في حين أن العديد من التحركات الاستراتيجية، مثل التجنب والسيطرة والتعاون، يمكن أن تقلل من حالات عدم اليقين. يؤدي التقليل من المخاطر إلى عواقب مؤسفة تؤثر عادة على الأصول الملموسة وغير الملموسة، والأسوأ من ذلك، دفع الشركة إلى الإفلاس.

وبحسب الدراسات السابقة تواجه الشركات الصغيرة والمتوسطة الحجم ستة أنواع رئيسية من المخاطر، وهي على النحو التالي: "مخاطر أسعار الفائدة، ومخاطر أسعار المواد الخام، ومخاطر الأعمال الإلكترونية والتكنولوجية، ومخاطر سلسلة التوريد، ومخاطر النمو، ومخاطر الإدارة والموظفين". وتركز هذه الدراسة على "الأعمال التجارية الإلكترونية والمخاطر التكنولوجية" في الشركات الصغيرة والمتوسطة الحجم باعتبارها المخاطر الرئيسية، وتحديدًا إدارة مخاطر الأمن السيبراني. على الرغم من أن هناك العديد من الدراسات السابقة حول إدارة المخاطر في الشركات الصغيرة والمتوسطة الحجم، إلا أن هناك القليل المتعلق بإدارة مخاطر الأمن السيبراني في الشركات الصغيرة والمتوسطة الحجم.

وبالتالي شهد موضوع الإفصاح عن إدارة مخاطر الأمن السيبراني اهتماماً كبيراً من قبل العديد من الهيئات المهنية في الدول المختلفة من خلال إصدار العديد من الإرشادات والتقارير المهنية لدعم إفصاح الشركات عن إدارة مخاطر الأمن السيبراني (SEC,2011,2018; AICPA,2017; CSA,2017; CPA–Canada,2017). اما فيما يتعلق بالوضع في مصر, وضع المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء وبرئاسة وزير الاتصالات وتكنولوجيا المعلومات في عام 2017 استراتيجية وطنية للأمن السيبراني في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري في مجال الأمن السيبراني (الهيئة الوطنية للأمن السيبراني, 2019؛ الاستراتيجية الوطنية للأمن السيبراني, 2017). ومع ذلك, لا يوجد اي معايير او ارشادات منظمة للإفصاح عن إدارة مخاطر الأمن السيبراني, كما لا يوجد متطلبات من سوق الأوراق المالية للشركات المقيدة بالبورصة المصرية بتقديم إفصاح عن إدارة مخاطر الأمن السيبراني.

واهتمت ايضاً العديد من الدراسات السابقة (Frank et al., 2019; Cheng & Walton, 2019; Yang et al, 2020; Tuson, 2021; Kamiya et al, 2021; Perols & Murthy, 2021) بدراسة تأثير الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين وأصحاب المصالح, وكذلك علي الأداء المالي للشركات. ولكن يأخذ علي هذه الدراسات أن معظمها تم في أسواق رأس المال المتقدمة والمتطورة, ولذلك يهدف هذا البحث إلي دراسة أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في سوق الأوراق المالية المصرية النامية.

2. مشكلة البحث

علي الرغم من زيادة اهتمام الهيئات المنظمة والرقابية في العديد من الدول المختلفة بإدارة مخاطر الأمن السيبراني والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني, وذلك لما له تأثير علي أمن المعلومات وزيادة شفافية التقارير والحد من عدم تماثل المعلومات ومن ثم التأثير علي قرارات الاستثمار في الشركات, الا انه لم يحظى بالاهتمام الكافي من قبل القوانين والمعايير المصرية وقواعد القيد والشطب في بورصة الأوراق المصرية. وايضاً لم تتناول الأبحاث والدراسات السابقة المصرية بشكل كافي أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيراني وأثره علي قرارات الاستثمار في أسهم الشركات المقيدة بالبورصة المصرية. ويعتقد الباحث أ، الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني له أثر إيجابي علي كفاءة قرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية.

في ضوء ما سبق يمكن تلخيص مشكلة البحث في التساؤلات التالية:

2-1 ما المقصود بإدارة مخاطر الأمن السيبراني وأهميتها – وما أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني؟

2-2 ما طبيعة العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في أسهم الشركات المقيدة؟

2-3 ما هو أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيراني علي قرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم في البيئة المصرية؟

3.أهداف البحث

يتجسد الهدف الرئيسي للبحث في دراسة وتحليل تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني، وأهميته, والمنهجية التي يجب أن تتبعها الشركات لتحسين شفافية المعلومات والحد من عدم تماثل المعلومات، ودراسة وتحديد العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في أسهم الشركات، وما أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات

الاستثمار في الشركات المصرية الصغيرة ومتوسطة الحجم. وذلك سعياً نحو تحقيق الأهداف الفرعية التالية:

3-1 اختبار العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار.

3-2 اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في أسهم الشركات المصرية الصغيرة ومتوسطة الحجم.

3-3 تقديم التوصيات والمقترحات التي تعزز دور تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في الشركات المصرية الصغيرة والمتوسطة الحجم.

4.أهمية ودوافع البحث

تنبع أهمية البحث من حقيقة وجوهرية المشكلة التي يتناولها بشأن تحديد الآثار الايجابية والسلبية للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، والذي يستهدف تحسين قرارات الاستثمار في أسهم الشركات بما يضفي مزيد من الدقة والمصداقية والملاءمة للمعلومات المحاسبية التي يتم الإفصاح عنها بالشركات الصغيرة والمتوسطة الحجم، ويمكن عرض أهمية البحث من الجانبين العلمي والعملي على النحو التالي:

4-1 الأهمية العلمية

- تزايد التغيرات التي طرأت على الأنظمة والممارسات المحاسبية والمراجعة بشكل عام والتي ارتبطت بمخاطر الأمن السيبراني في الآونة الأخيرة، الأمر الذي دفع الأكاديميين والمهتمين بهذا المجال والقائمين على التنظيم إلى المطالبة بوجود قواعد وسياسات محاسبية ومعايير مراجعة موحدة تلقى القبول العام على المستوى الدولي بشأن إدارة مخاطر الأن السيبراني.
- تزايد الاهتمام بتحسين جودة المعلومات المفصح عنها من الشركات الصغيرة والمتوسطة الحجم والتي تسهم في استقرار الشركات وتعزز من قدرة الشركات الصغيرة والمتوسطة على الاستمرار في ظل ظروف عدم الاستقرار الاقتصادي.
- تعزيز قدرة المستثمرين وأصحاب المصالح في الشركات الصغيرة والمتوسطة الحجم على فهم المعلومات المفصح عنها من تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني والتي تعمل علي زيادة شفافية المعلومات والحد من عدم تماثلها.

4-2 الأهمية العملية

- يساعد تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني في الشركات الصغيرة والمتوسطة الحجم في تعزيز جودة المعلومات المحاسبية الملاءمة المفصح عنها بما يفي بمتطلبات المستثمرين وأصحاب المصالح من جانب، والهيئة العامة للرقابة المالية من جانب أخر.
- تزايد إدراك المستثمرين في الشركات الصغيرة والمتوسطة الحجم لأهمية وجود معلومات محاسبية دقيقة ومتنوعة وموحدة وتتميز بمستوي مرتفع من الجودة، تمكنهم من اتخاذ قرارات مناسبة بشكل يعكس ربحية استثماراتهم.
- تزايد حاجة الشركات الصغيرة والمتوسطة الحجم إلى معلومات مالية وغير مالية بجودة وشفافية عالية، الأمر الذي يمكنهم من تجنب المخاطر الناشئة وإدارتها بشكل مناسب حال حدوثها.

5. منهج البحث

في ضوء مشكلة البحث وسعياً نحو تحقيق أهدافه واختبار فروضه اعتمد الباحث على كل من المنهج الاستقرائي والاستنباطي، وذلك على النحو التالي:

5-1 المنهج الاستقرائي: في ظل هذا المنهج اهتم الباحث بدراسة وتحليل ما ورد بالقرارات المصرية والمبادئ والمعايير المحاسبية والدراسات الأجنبية المرتبطة بمتغيرات البحث، وكذلك التقارير الدورية والإصدارات المهنية المتخصصة في تقارير الإفصاح عن إدارة مخاطر الأمن السيبراني، فضلاً عن الرجوع إلى تعليمات وقرارات رئيس مجلس الوزراء فيما يخص بمتطلبات وتنظيم الأمن السيبراني في مصر. وذلك بهدف عرض وتحليل متطلبات تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني وتحديد أهم التحديات التي تواجه الشركات المصرية الصغيرة والمتوسطة الحجم بشأن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.

5-2 المنهج الاستنباطي: وفقاً لهذا المنهج حرص الباحث على اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم في البيئة المصرية تجريبياً، من اختبار هذه العلاقة علي بيانات الشركات محل الدراسة.

6. فروض البحث

في ضوء نتائج الدراسات السابقة واتفاق العديد من الدراسات علي أن هناك علاقة إيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية، علي الرغم من اختلاف نتائج بعض الدراسات، وفي ضوء تساؤلات البحث وسعياً نحو تحقيق أهدافه، واستناداً على استقراء الدراسات السابقة يمكن صياغة فروض البحث على النحو التالي:

H_1: يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني جوهرياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية.

H_2: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر.

H_3: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر.

H_4: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر.

7. نطاق وحدود البحث

7-1 حدود منهجية (موضوعية): يرتكز البحث على عرض وتحليل متطلبات تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني، وكذلك القوانين والإرشادات الدولية المنظمة لتقرير الإفصاح عن إدارة مخاطر الأمن السيبراني.

7-2 حدود مكانية: تتمثل في الشركات الصغيرة والمتوسطة الحجم المصرية سواء كانت تقوم بالإفصاح عن تقرير إدارة مخاطر الأمن السيبراني ام لا.

7-3 حدود زمنية: تتمثل في استخراج وتحليل البيانات الخاصة بمتغيرات البحث للشركات الصغيرة والمتوسطة الحجم المصرية محل الدراسة التجريبية بواقع (261) مشاهدة لعدد 253 شركة صغيرة ومتوسطة الحجم، وذلك بالاعتماد على القوائم المالية لهذه الشركات.

8. خطة البحث

في ضوء مشكلة البحث, وسعيا نحو تحقيق أهدافه, وتجسيدا لاختبار فروضه واعتمادا علي منهجه لاستخلاص أهم النتائج وتقديم التوصيات تم تقسيم هذا البحث علي النحو التالي:

8-1 تقرير إدارة مخاطر الأمن السيبراني – المفهوم والأهمية.

8-2 تحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم.

8-3 الدراسة التجريبية للشركات الصغيرة والمتوسطة الحجم محل الدراسة.

8-4 نتائج اختبار فروض البحث.

8-5 التوصيات والدراسات المستقبلية.

8-1 إدارة مخاطر الأمن السيبراني: المفهوم والأهمية

تتمثل الأهداف العامة للأمن السيبراني في الحفاظ علي سرية المعلومات وسلامتها وتوافرها. حيث يصف المعهد الأمريكي للمحاسبين القانونيين (2017) AICPA الأمن السيبراني بأنه عملية تنفيذ وتشغيل الضوابط وأنشطة إدارة المخاطر الأخرى لحماية المعلومات والأنظمة من الأحداث الأمنية التي يمكن أن تعرضها للخطر عندما لا يتم منع الأحداث الأمنية، والتعافي من تلك الأحداث في الوقت المناسب. كما يعرف الأمن السيبراني أنه مجموعة من التقنيات والعمليات والممارسات التي تحمي وتضمن حماية أصول المنشأة (2017) No & Vasarhelyi. كما عرفه (2014).Craigen et al بأنه تنظيم وجمع الموارد والعمليات والهياكل التي يتم استخدامها لحماية الفضاء الإلكتروني والأنظمة الأخرى التي تدعم الفضاء الإلكتروني من الهجمات والحوادث الإلكترونية.

ونتيجة زيادة استخدام الانترنت والحوسبة السحابية في الشركات زادت حوادث الأمن السيبراني مما أدى إلي ضرر كبير علي الشركات التي تتعرض لحوادث الاختراق، وقد يصل الضرر إلي فقد الشركة لسمعتها (Rosati et al,2020). فوفقا لتقرير (2017) CISCO فإن أكثر من 20% من الشركات التي تتعرض لاختراق أمني تواجه خسارة كبيرة في الإيرادات وانخفاضا في عدد عملائها وخسارة حصتها السوقية، وقد بلغت اجمالي الخسائر حوالي 17 مليون دولار أمريكي لكل شركة.

كما حدد تقرير (2018) Kaspersky أهم الدول العربية التي تعرضت لهجمات سيبرانية لأنظمتها وجاءت مصر في المركز الثالث بنسبة 57%. كما أشار تقرير (2020) COSO إلي أن 90% من الشركات الأمريكية التي انخرطت في التحول الرقمي تعرضت لمخاطر هجمات الكترونية، وزاد اهتمامها بإدارة مخاطر الأمن السيبراني.

ولا ترتبط مخاطر الأمن السيبراني بالشركات الكبيرة فقط، ولكن تزداد تلك المخاطر في الشركات الكبيرة والمتوسطة والصغيرة. فعلي الرغم من أن الشركات الكبيرة تكون أكثر عرضة للهجمات الالكترونية، إلا أن الشركات المتوسطة والصغيرة تكون أيضا عرضة لهذه الهجمات الالكترونية نظرا لقلة امكانياتها وضعف وسائل الحماية فيها (2018) ISCA. وأوضحت دراسة (2019) Bourdon أن مرتكبي الهجمات الإلكترونية يخترقون الأمن السيبراني للشركات بشكل متكرر ويسرقون البيانات السرية للحصول علي مزايا مالية سريعة وغير قانونية, ويتضح ذلك من خلال سلسلة الاختراقات التي تعرضت لها شركة Yahoo Inc في أواخر عام 2016 عندما تمكن أحد مرتبكي الهجمات الإلكترونية من الوصول إلي شبكة الشركة وسرقة معلومات من حسابات ما لا يقل عن 500 مليون مستخدم.

وفي هذا الصدد توقعت دراسة Lord (2018) أنه بحلول عام 2020 من المتوقع أن ثلث معلومات الشركات الأمريكية ستكون مخزنة علي سحابة، وخلال خمس سنوات سيكون هناك 50 مليار جهاز متصل بالسحابة. وهذا يمثل فرصة للقراصنة ومجرمي الانترنت لاختراق البيانات الهامة للشركات، ففي الولايات المتحدة الأمريكية تم الاعلان عن 4500 حادثة اختراق لبيانات الشركات خلال الفترة من 2005 الي 2018. كما أشار Fettetti et al (2021) إلي أن ممارسات الأمن السيبراني قد تتعرض للعديد من التلاعب أو الاختراق ليس فقط من مصادر خارجية، ولكن أيضا من قبل الأشخاص المصرح لهم بالتعامل مع النظام، لذلك يجب أن يكون هناك رقابة علي أنظمة الأمن السيبراني لضمان اكتشاف التصرفات غير القانونية والهجمات الالكترونية الداخلية.

ومع استمرار زيادة حوادث الأمن السيبراني يزداد قلق أصحاب المصالح فيما يتعلق بالنتائج المترتبة علي تلك الحوادث، والتي قد تصل إلي فقد الحصة السوقية للشركة وخروجها من السوق. ونتيجة لذلك زاد طلب المستثمرين على معلومات الأمن السيبراني للشركات. كما زاد اهتمام الشركات بتجنب تلك الحوادث من خلال زيادة ممارسات إدارة مخاطر الأمن السيبراني، والإفصاح عن تلك الممارسات لأصحاب المصالح (Eaton et al.,2019).

وقد زاد الإفصاح عن مخاطر الأمن السيبراني للشركات بشكل كبير علي مر السنين وهو مدفوع بعوامل كثيرة مثل زيادة مخاطر الأمن السيبراني وتوجيهات هيئة البورصة الأمريكية وحجم الشركة، وأوضحت دراسة Bourdon (2019) أن الإفصاح عن إدارة مخاطر الأمن السيبراني يعد منهجاً جديداً نسبياً لإفصاحات الشركات, ونظراً للطبيعة البارزة للهجمات الإلكترونية علي الشركات فقد زاد الطلب علي المعلومات المتعلقة بالأمن السيبراني والحاجة إلي تسهيل المحادثات القوية حول هذه الموضوعات بشكل كبير عبر مجموعات أصحاب المصلحة الرئيسين.

وفيما يتعلق بمفهوم إدارة مخاطر الأمن السيبراني، فقد عرفها Perols (2019) علي أنها مجموعة من السياسات والعمليات والاجراءات الرقابية المصممة لحماية المعلومات والأنظمة الالكترونية من الحوادث الأمنية[1] التي تعرض أمن الشركة السيبراني لمخاطر عدم تحقيق أهدافه، كما تساعد تلك الإجراءات علي اكتشاف الهجمات الأمنية والاستجابة لها والتخفيف من آثارها، وسرعة التخلص من الآثار السلبية الناتجة عن الهجمات التي لا يمكن منعها.

كما عرفت الهيئة الوطنية للأمن السيبراني (2018) مخاطر الأمن السيبراني بأنها المخاطر التي تهدد عمليات الشركة بما في ذلك رؤية الشركة، أو رسالتها أو إدارتها أو صورتها أو سمعتها أو أصولها، بسبب

إمكانية الوصول غير المصرح به أو سوء الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات.

وفي نفس السياق أكد الدليل التنظيمي للأمن السيبراني (2020) علي أن إدارة مخاطر الأمن السيبراني تشتمل علي خطوتين هما: الخطوة الأولي, إعداد وتنفيذ منهجية مناسبة لتحديد مخاطر الأمن السيبراني وتحليلها وتقييمها لحماية الأصول المعلوماتية للشركة؛ بينما الخطوة الثانية، إعداد وتنفيذ منهجية مناسبة لمراقبة مخاطر الأمن السيبراني ومعالجة المخاطر التي تم تحديدها في الخطوة الأولي ومتابعة خطط المعالجة.

ومما سبق يعتقد الباحث إلي أن الأمن السيبراني، يشمل حماية الأنظمة والشبكات والبرامج وأصول المنشأة من الهجمات والحوادث الإلكترونية التي يمكن أن تؤثر علي أداء عملها بشكل فعال وكفء، وذلك من أجل تحقيق أهداف الحفاظ علي سرية المعلومات وسلامتها وتوافرها.

وفيما يتعلق بإطار إعداد تقرير للإفصاح عن إدارة مخاطر الأمن السيبراني, هدفت دراسة Yang el al.,(2020) إلي البحث عن مدي إدراك المستثمرين لأهمية إطار إعداد تقرير إدارة مخاطر الأمن السيبراني الذي قدمه (AICPA) في عام 2017, وذلك من خلال دراسة تجريبية أجريت علي 226 مستثمر غير محترف في الولايات المتحدة الأمريكية. وتوصلت الدراسة إلي أن إطار إعداد تقرير إدارة مخاطر الأمن السيبراني الذي قدمه المعهد الأمريكي للمحاسبين القانونيين يمكن الشركات من الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني طبقاً لهذا الإطار كان له تأثير إيجابي علي تحسين قرارات المستثمرين, وساهم في زيادة ثقة المستثمرين في تلك الشركات.

وفي نفس السياق, توصلت دراسة Kelton & Pennington (2020) من خلال دراسة تجريبية تمت علي عينة مكونة من 120 مستثمر غير محترف في الولايات المتحدة, إلي أن الإفصاح الاختياري عن تقرير إدارة مخاطر الأمن السيبراني له تأثير إيجابي علي قرارات المستثمرين.

ولقد اتجهت الهيئات والمنظمات المهنية في العديد من دول العالم إلي إصدار العديد من الإرشادات التي تنظم وتطور الإفصاح الاختياري عن تقرير إدارة مخاطر الأمن السيبراني، بهدف مساعدة أصحاب المصالح علي تقييم أداء الشركات في مجال الأمن السيبراني. وذلك من خلال العديد من الإصدارات في هذا الصدد.

1- **الحوادث الأمنية:** هي مجموعة الأنشطة ذات التأثير السلبي علي المنظمة والتي تهدد أمن أنظمة الحاسب والشبكات (Perols ,2019).

في الولايات المتحدة الأمريكية، أصدرت هيئة البورصة الأمريكية في عام 2011 توجيهها الأول بشأن التزامات الإفصاح المتعلقة بمخاطر وحوادث الأمن السيبراني لمساعدة الشركات في تقييم ما يجب أن تقوم به من إفصاحات في هذا المجال إن وجدت وتنص التوجيهات علي أنه في حين لم يتم فرض متطلبات إفصاح صريحة تتعلق بمخاطر الأمن السيبراني والحوادث الإلكترونية فإن الإفصاح عن مخاطر وقضايا الأمن السيبراني يتفق مع مشاركة المعلومات الدقيقة في الوقت المناسب للمساعدة في اتخاذ قرارات الاستثمار (2022) ,.Barry et al. كما قدم المعهد الأمريكي للمحاسبين القانونيين (2017) AICPA في أبريل 2017 إطاراً لإعداد تقرير إدارة مخاطر الأمن السيبراني، لإرشاد الشركات ودعمها في الإفصاح الاختياري عن مخاطر الأمن السيبراني, وذلك من خلال تمكين جميع الشركات – في مختلف الصناعات – من تبني نهج استباقي لإدارة مخاطر الأمن السيبراني, والتقرير عنها وتوصيل تلك الأنشطة ونتائجها إلي أصحاب المصالح ولدعم الإطار تم إصدار مجموعتين من المعايير لوصف أهداف عمليات وضوابط الأمن السيبراني الفعالة التي يجب علي الشركات تصميمها وتنفيذها للحصول علي برنامج قوي وفعال لإدارة مخاطر الأمن السيبراني. حيث تشمل المجموعة الأولي علي مراجعة قواعد الإفصاح عن مشاكل الأمن السيبراني, بينما تشمل المجموعة الثانية علي السياسات والإجراءات الخاصة بالرقابة علي الإفصاح عن إدارة مخاطر الأمن السيبراني. وعلي نفس السياق, أصدرت لجنة البورصة والأوراق المالية الأمريكية في عام 2018 دليلا يتضمن إرشادات للشركات المقيدة بالبورصة يتعلق بمتطلبات الإفصاح عن الأمن السيبراني.

وفي عام 2016، أصدر مركز جودة المراجعة (CAQ) التابع لـ (AICPA) منشوراً يشير إلي دور المراجعين الخارجيين فيما يتعلق بمخاطر الأمن السيبراني للشركات, ويشتمل مراجعة القوائم المالية ونظم الرقابة الداخلية علي التقارير المالية, والإفصاحات (Calderon & Gao,2021). أما مجلس (PCAOB) فقد أشار إلي أنه يجب علي المراجعين ألا يقوموا فقط بتقييم تأثير الحادث علي القوائم المالية للشركة ولكن يقوموا ايضاً بتقييم مخاطر أحداث الأمن السيبراني حتي لو لم تحدث مثل هذه الأحداث بعد Calderon (&) Gao,2021.

وفي كندا, قدم معهد المحاسبين القانونيين الكنديين وكذلك هيئة سوق الأوراق المالية الكندية عام 2017 إرشادات للشركات المقيدة بالبورصة تتعلق بكيفية الإفصاح عن مخاطر الأمن السيبراني، والإفصاح عن الآثار المحتملة لحوادث الأمن السيبراني، والإفصاح عن أنشطة الحوكمة للتخفيف من مخاطر وحوادث الأمن السيبراني. ويتم ذلك في القوائم المالية أو في مناقشات وتحليلات الإدارة من أجل توضيح الأمور ذات الأهمية النسبية والاتجاهات والمخاطر التي من المحتمل أن تؤثر علي أداء الشركات في المستقبل, وكذلك مدي تأثير حوادث ومخاطر الأمن السيبراني علي البيانات المالية للشركات.

وفيما يتعلق بالوضع في مصر، فقد نصت المادة (31) من الدستور المصري في يناير 2014 علي أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه, علي النحو الذي ينظمه القانون". وبناءً علي ذلك تم وضع الاستراتيجية الوطنية للأمن السيبراني (2017-2021) من قبل المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء وبرئاسة وزير الاتصالات وتكنولوجيا المعلومات. وبناء علي ذلك، تم وضع الاستراتيجية الوطنية للأمن السيبراني ضمن رؤية الدولة المصرية (2030) ويتمثل الهدف الاستراتيجي لها في مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة. وتشمل الاستراتيجية علي العناصر الآتية:

1- التحديات والأخطار السيبرانية: والتي تتمثل في خطر اختراق وتخريب البنية التحتية للاتصالات وتكنولوجيا المعلومات وخطر الإرهاب والحرب السيبرانية وخطر سرقة الهوية الرقمية والبيانات الخاصة.
2- أهم القطاعات الحيوية المستهدفة: وتشمل بالترتيب, قطاع الاتصالات وتكنولوجيا المعلومات, قطاع الطاقة وقطاع الخدمات الحكومية وقطاع النقل والمواصلات وقطاع الصحة وخدمات الإسعاف العاجل وقطاع الإعلام والثقافة، بالإضافة إلي المواقع الرسمية للدولة والقطاعات ذات التأثير علي النشاط الاقتصادي مثل: التجارة والصناعة والزراعة والري والتعليم بمختلف مستوياته والاستثمار والسياحة.
3- العناصر الرئيسية لخطورة التهديدات السيبرانية: استناداً إلي تقنيات متقدمة ومتطورة, وسرعة وسهولة انتشارها واتساع نطاق تأثيرها.
4- ركائز الاستعداد الاستراتيجي لمواجهة الأخطار السيبرانية: الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي, الإطار التشريعي، الإطار التنظيمي والتنفيذي, البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني وتنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات والتعاون مع الدول الصديقة والمنظمات الدولية والاقليمية ذات الصلة والتوعية المجتمعية.
5- آلية التنفيذ في تشكيل المجلس الأعلى للأمن السيبراني: لحماية البنية التحتية للاتصالات وتكنولوجيا المعلومات تحت اشراف وزارة الاتصالات وتكنولوجيا المعلومات وبرئاسة وزير الاتصالات والمجلس يتبع مجلس الوزراء من خلال وضع استراتيجية وطنية للأمن السيبراني والإشراف علي تنفيذها مع ضرورة تحديثها في ضوء التطورات التقنية المتلاحقة. ويمثل في المجلس الأطراف المعنية بالأمن القومي وبإدارة وتشغيل البنية التحتية في القطاعات الحيوية والمرافق العامة، وذو الخبرة في القطاع الخاص والجهات التعليمية والبحثية. وقد بدأ المجلس عمله التمهيدي في يناير 2015 وقام رئيس

مجلس الوزراء باعتماد تشكيل المكتب التنفيذي للمجلس ولجنته الفنية وتوصيف مهامه في يونيو 2016.

وفيما يتعلق بأهمية ادارة مخاطر الأمن السيبراني, أشار تقرير ISCA (2018) إلي أن تقييم مخاطر الأمن السيبراني لا يقل أهمية عن تقييم المخاطر المرتبطة بالتقارير المالية، فالحوادث الالكترونية يترتب عليها العديد من الخسائر المالية، والتي تنعكس علي بيانات التقارير المالية. هذا بالإضافة إلى الخسائر غير المالية. لذلك يجب أن يهتم مراقب الحسابات بفهم ممارسات الشركة فيما يتعلق بإدارة مخاطر الأمن السيبراني حتي يكون قادرا علي تحديد مخاطر التحريفات الجوهرية في القوائم المالية.

ونتيجة لأهمية إدارة مخاطر الأمن السيبراني تم تطوير إطار COSO (2017) لإدارة المخاطر لمواكبة التحول الرقمي، وذلك حتي يكون صالحاً لإدارة المخاطر السيبرانية، وحاجة الشركات لتحسين مدخل إدارة المخاطر المرتبطة بالأمن السيبراني لتلبية متطلبات بيئة الأعمال الحديثة. هذا وقد تم تطوير إطار إدارة مخاطر الأمن السيبراني من عدة أبعاد لتركيز الاهتمام على أهمية الأخذ في الاعتبار إدارة المخاطر عند وضع الاستراتيجية، وأداء الأعمال. كما يوفر الإطار نظرة ثاقبة عن أهمية إدارة المخاطر السيبرانية عند وضع وتنفيذ الاستراتيجية، ويوفر فهم لتأثير المخاطر علي الأداء من خلال تحسين التوافق بين المخاطر والأداء.

وفيما يتعلق بمردود ادارة مخاطر الأمن السيبراني علي الشركة, أشار Havakhor et al (2020) إلي أن الافصاح عن إدارة مخاطر الأمن السيبراني من شأنه الحد من عدم تماثل المعلومات فيما يتعلق بالمخاطر الأساسية للشركة، ويقلل من تكلفة التمويل بالاقتراض. كما يساهم في تحسين مقاييس الأداء، مثل العائد علي الأصول والعائد علي المبيعات. كما أن الإفصاح عن ممارسات الشركة للأمن السيبراني يعزز من اهتمام المحللين الماليين بالشركة ويزيد من الاستثمارات في الشركات ويخفض تكلفة رأس المال.

مما سبق يتضح أن الإفصاح عن إدارة مخاطر الأمن السيبراني أصبحت تمثل أهمية بالغة لكل شركة تتبني التحول الرقمي. فيجب على تلك الشركات إدارة والإفصاح عن مخاطر الأمن السيبراني، وأن تعتبره من أهم أولوياتها نظرا لأهمية المعلومات المخزنة على الأنظمة الالكترونية، والتي ينتج عن اختراقها خسارة كبيرة للشركة قد تصل إلى فقد عملائها والإضرار بسمعتها وخروجها من السوق. وتتمثل أهمية إدارة الأمن السيبراني في حماية بيانات الشركات والتخفيف من أثار حوادث الأمن السيبراني اللاحقة. كما يترتب على الإفصاح عن إدارة مخاطر الأمن السيبراني العديد من المنافع لكل من الشركة ومراقب الحسابات وأصحاب المصالح.

وفيما يتعلق بمراحل الإفصاح عن إدارة مخاطر الأمن السيبراني، فتتمثل في خمس مراحل، وهي: تحديد المخاطر وقياسها، تصميم واختبار نظام مراقبة الأمن السيبراني، اختبار الفعالية التشغيلية لرقابة الأمن السيبراني، الإفصاح عن ممارسات إدارة مخاطر الأمن السيبراني، تقديم خدمة التوكيد علي تقارير الإفصاح عن إدارة مخاطر الأمن السيبراني حال تكليف مراقب الحسابات بتلك الخدمة التصديقية وإن كان يمكن أن يقدم خدمة استشارية بشأن إدارة مخاطر الأمن السيبراني (Eaton et al.,2019).

وعلي الرغم من زيادة الاهتمام بالإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في الشركات، إلا أنه لا يوجد متطلبات أو معايير منظمة ومحددة من المشرعيين وواضعي المعايير لتلك الممارسات. وعلي الرغم من عدم وجود إطار شرعي لتلك الممارسات إلا أنه يوجد بعض الارشادات التي قدمتها بعض الهيئات لمساعدة الشركات في الإفصاح عن إدارة مخاطر الأمن السيبراني.

وكاستجابة لزيادة طلب أصحاب المصالح عن معلومات الأمن السيبراني للشركات اصدر AICPA بالتعاون مع مجلس معايير المراجعة ASB اطاراً اختيارياً للتقرير والتوكيد عن مخاطر الأمن السيبراني كوسيلة للشركات لتوصيل جهودها فيما يتعلق بإدارة مخاطر الأمن السيبراني إلي أصحاب المصالح.

ومما سبق يعتقد الباحث إلي أن زيادة اهتمام الشركات بالإفصاح عن إدارة مخاطر الأمن السيبراني كنتيجة زيادة طلب أصحاب المصالح علي معلومات أكثر عن الأمن السيبراني للشركات. كما يمكن أن يلعب تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني دوراً هاماً في مساعدة المستثمرين في القرارات المتعلقة بالاستثمار في أسهم الشركات.

وفيما يتعلق بإطار الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني, تشير الزيادة الكبيرة في عدد شركات الأمن السيبراني خلال السنوات العشر الماضية إلى خطورة التحديات السيبرانية التي تواجهها الشركات. بالإضافة إلى إجراء عمليات المراجعة الروتينية، يمكن لشركات المحاسبة أيضًا تقديم المشورة بشأن جميع جوانب إدارة مخاطر الأمن السيبراني. من المستحيل المبالغة في أهمية التعاون المتزايد بين المراجعين الداخليين ومحترفي نظم المعلومات في حماية أصول الشركات. يعد إطار إعداد تقارير إدارة مخاطر الأمن السيبراني الخاص بـ AICPA استجابة لهذا التعاون، وذلك باستخدام المكونات الرئيسية الثلاثة التالية لمساعدة أصحاب المصلحة على مراقبة برنامج إدارة مخاطر الأمن السيبراني للكيان (AICPA,2017):

- وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني في الشركة. حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة وللمحاسبين القانونيين لتقييم الوصف. ولتزويد المستخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة.

- تأكيد الإدارة على أن وصف برنامج الكيان يتوافق مع معايير الوصف الخاصة بـ AICPA وأن الضوابط التي تنفذها الإدارة يمكن أن تحقق أهداف الأمن السيبراني للكيان بشكل فعال. وترتكز هذه الأهداف على مجموعة من معايير الرقابة المناسبة، مثل معايير خدمات الثقة (معايير الأمان والتوافر والسرية).
- رأي المراجع في إفصاحات الإدارة وفعالية ضوابط الشركة (تقرير ضوابط النظام والتنظيم للأمن السيبراني).

وفيما يتعلق بمحددات الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني, فتناولت عدد قليل من الدراسات محددات الإفصاح عن مخاطر الأمن السيبراني (Brown et al., 2018; SEC, 2018; Walton et al.,2021; Cheong et al. 2021), فأشارت دراسة Walton et al.,(2021) إلي أنه علي نفس سياق المخاطر الأخرى التي يتم الإفصاح عنها، يهدف الإفصاح عن مخاطر الأمن السيبراني إلي تقليل عدم تماثل المعلومات، وخفض التكاليف القانونية وتكاليف السمعة اللاحقة. ومع ذلك، علي الرغم من أن هناك مطالبة من الشركات لتقديم توصيفات نوعية للمخاطر في قسم منفصل في التقارير السنوية، إلا أن لا يوجد شرط واضح لتقديم تقدير كمي عن المخاطر المفصح عنها. وبالإضافة إلي ذلك، يحتفظ المديرين بالسلطة التقديرية في تحديد ماذا وكيف وكم الإفصاحات عن مخاطر الأمن السيبراني. وعلي نحو مماثل, توصلت دراسة Cheong et al.,(2021) من خلال دراسة مسحية أجرتها علي عدد من الشركات إلي أنه يمكن تصنيف إفصاحات مخاطر الأمن السيبراني إلي مجموعات من عوامل الخطر علي النحو التالي: التحكم في الحوادث وتخفيف المخاطر، والمخاطر التشغيلية، والمخاطر المتعلقة بالعميل، والمخاطر المتعلقة بالتعاقدات، ومخاطر استمرارية الأعمال, ومخاطر نظم الدفع، ومخاطر أمان الشركات، ومخاطر وموفري البرامج من الجهات الخارجية والتوكيد. وتوصلت الدراسة ايضاً أنه يمكن تصنيف كل موضوع خطر داخل كل عامل إلي مكونات الضعف والثغرات الأمنية والرقابة، ويمثل مكون الضعف والثغرات الأمنية مخاطر الأمن السيبراني التي تواجهها الشركات، بينما يشير عنصر الرقابة إلي الضمانات أو الإجراءات المضادة التي تكتشف المخاطر أو تتصدي لها أو تعمل علي تقليلها. كما أشار Brown et al., (2018) أن الشركات تعمل علي تعديل الإفصاحات اللاحقة لإدراج المزيد من العناصر المتعلقة بالأمن السيبراني. وتوصلت الدراسة إلي أن اهتمام المنظمين بالأمن السيبراني يمكن أن يكون آلية رقابية فعالة في مجالات الإفصاح عن مخاطر الأمن السيبراني.

وفيما يتعلق بالمحتوي المعلوماتي لتقرير الإفصاح عن إدارة مخاطر الأمن السيبراني, فقد تناولت العديد من الدراسات (e.g., Berkman et al., 2018; Ettredge et al. 2018; Li et al., 2018; Tan & Yu, 2018;Cheng & Walton, 2019; Frank et al.,2019; Héroux&

Fortin,2020; Kelton & Pennington, 2020; Calderon & Gao, 2021; Walton et al.,2021) آثار إفصاحات الأمن السيبراني, علي وجود آثار عملية كبيرة, تقدم الدراسات أدلة غير حاسمة حول فعالية الإفصاح عن مخاطر الأمن السيبراني. من ناحية أخري, قد تؤدي زيادة الإفصاح عن مخاطر الأمن السيبراني إلي تقليل عدم تماثل المعلومات، كما يخصص السوق قيمة أعلي للشركات ذات الجودة العالية والإفصاحات ذات الصلة بالأمن السيبراني. علاوة علي ذلك، قد توصلت الدراسات السابقة إلي وجود ارتباط إيجابي بين الإفصاح عن مخاطر الأمن السيبراني وجذب الاستثمارات. ولكن من ناحية أخري, عندما تفصح الشركات عن المخاطر المتعلقة بالأمن السيبراني، فإن المخاطر التي تم الإفصاح عنها قد تجذب المتسللين من غير قصد إلي أنظمة معلومات الشركة. ومع ذلك، فأن محتوي تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني مفيد في التنبؤ بحوادث الأمن السيبراني في المستقبل.

ويعتقد الباحث أن تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني سلاح ذو حدين لأنه يمكن من تقليل عدم تماثل المعلومات ولكنه في المقابل يزيد ايضاً من احتمال وقوع حوادث الأمن السيبراني في المستقبل. وبالتالي، فإن استكشاف أثر الإفصاح عن إدارة مخاطر الأمن السيبراني يمكن المنظمات المهنية من اكتشاف الفعالية والتحديات والعواقب المحتملة غير المقصودة للإفصاح عن إدارة مخاطر الأمن السيبراني.

2-8 تحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم, واشتقاق الفروض

اكتسبت قضايا المحاسبة المتعلقة بالإفصاح عن مخاطر الأمن السيبراني اهتماماً كبيراً وواضحاً من واضعي معايير المحاسبة ومكاتب المحاسبة والمراجعة الكبرى والجمعيات المهنية، ومع ذلك فأن عدداً محدوداً من الدراسات الأكاديمية التي تناولت الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في الأسهم. وبالرغم من ذلك، فأن هناك تضارب بين نتائج الدراسات السابقة حيث وجدت بعض الدراسات ردود فعل إيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار[1] في الأسهم (Spanos&Angelis,2016; Arcuri et al.,2018; Amir et al.,2018; Berkman et al.,2018; Arcuri et al.,2020), بينما وجدت البعض الآخر وجود ردود فعل سلبية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم (Gordon et al., 2011; Morse et al., 2011; Pirounias et al., 2014;Hinz et al., 2015; Modi et al.,2015; Amir et al., 2018).

قامت دراسة Spanos & Angelis (2016) بالبحث في أثر الإفصاح عن الأمن السيبراني للمعلومات علي أسعار الأسهم وذلك من خلال دراسة تحليلية لـ (45) دراسة سابقة. وتوصلت هذه الدراسة إلي أن غالبية هذه الدراسات (75.6%) تشير إلى وجود علاقة معنوية إيجابية لتأثير الأحداث الأمنية على أسعار أسهم الشركات.

اشارت دراسة Arcuri et al., (2018) أن إحدى القضايا التي نوقشت على نطاق واسع في السنوات الأخيرة هي الجرائم السيبرانية. حيث تنطوي انتهاكات الأمن السيبراني إمكانية الوصول إلى المعلومات وسلامتها وسريتها. لذلك هدفت هذه الدراسة إلي البحث في تأثير انتهاكات أمن المعلومات على عوائد الأسهم. وباستخدام منهجية دراسة الأحداث، توفر الدراسة أدلة تجريبية على تأثير إعلانات الهجمات السيبرانية على القيمة السوقية للشركات من عام 1995 إلى عام 2015. وتظهر النتائج أن عوائد السوق السلبية الكبيرة تحدث بعد الإعلان عن الهجمات السيبرانية. غالباً ما يعاني قطاع الكيانات المالية من تأثيرات سلبية أكبر من الشركات الأخرى، وتعد الهجمات السيبرانية هي الأكثر خطورة، خاصة بالنسبة للقطاع المالي.

وتوصلت دراسة Amir et al., (2018) إلي أنه يجب على الشركات الكشف عن المعلومات المتعلقة بالهجمات السيبرانية المادية. ومع ذلك، لأن المديرين لديهم حوافز لحجب المعلومات السلبية، ولأن المستثمرين لا يستطيعون اكتشاف معظم الهجمات السيبرانية بشكل مستقل، فقد تقوم الشركات بالإبلاغ عنها بشكل أقل. وباستخدام البيانات المتعلقة بالهجمات الإلكترونية التي كشفت عنها الشركات طوعًا، وتلك التي تم حجبها واكتشافها لاحقًا بواسطة مصادر من خارج الشركة، نقوم بتقدير مدى حجب الشركات للمعلومات المتعلقة بالهجمات الإلكترونية. اتضح أن الهجمات السيبرانية المحجوبة مرتبطة بانخفاض قدره 3.6% تقريبًا في قيم الأسهم في الشهر الذي تم اكتشاف الهجوم فيه، والهجمات المكشوفة بانخفاض أقل بكثير قدره 0.7%. تتوافق الأدلة مع عدم قيام المديرين بالكشف عن معلومات سلبية أقل من حد معين وحجب المعلومات المتعلقة بالهجمات الأكثر خطورة. وباستخدام ردود أفعال السوق تجاه الهجمات المحجوبة والمفصح عنها، فإننا نقدر أن المديرين يكشفون عن معلومات حول الهجمات الإلكترونية عندما يشك المستثمرون بالفعل في وجود احتمال كبير (40٪) لوقوع هجوم.

1- قرار الاستثمار: يقصد به استعداد المستثمرين للاستثمار في أسهم الشركة، واختيار بين بديلين أو أكثر من بين البدائل المتاحة وفق معيار العائد علي الاستثمار (شحاته، 2014).

كما وجدت دراسة Berkman et al., (2018) علاقة إيجابية بين أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني والقيم السوقية لأسعار الأسهم والوعي بالأمن السيبراني وقرارات الاستثمار. وتوصلت الدراسة ايضاً أن الأحداث السلبية في عمليات الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني مرتبطة بقيم السوق المنخفضة. وتتوافق نتائج هذه الدراسة مع نتائج دراسة Gordon et al., (2015) التي توصلت إلي أن الإفصاح للمستثمرين عن معلومات حول وعي الشركات بالأمن السيبراني يحظى بتقدير إيجابي من قبل السوق علي قرارات الاستثمار.

وهدفت دراسة Arcuri et al., (2020) إلي تحليل تأثير الهجمات السيبرانية على عوائد أسهم الشركات العاملة في قطاع الضيافة[1]. حيث تعد التقنيات الرقمية أدوات مهمة للتنمية المستدامة، ولكن إذا لم يتم التعامل معها بشكل مناسب، فمن المحتمل أن تعيق التقدم نحو الاستدامة. ومن بين الآثار السلبية، من الضروري النظر في المخاطر السيبرانية، التي تشكل مصدر قلق كبير اليوم، ولا سيما بالنسبة للصناعات التي تعمل مع البيانات الحساسة، مثل شركات السياحة. فـ يتعين على شركات الضيافة إدارة قضايا انعدام الأمن السيبراني والخصوصية الرقمية بشكل مناسب، لمنع الخسائر والمساهمة في النمو الاجتماعي والاقتصادي المستدام.

وباستخدام منهجية دراسة الأحداث، قدمت هذه الدراسة أدلة تجريبية حول تأثير الإعلانات عن 170 انتهاكًا لأمن المعلومات على القيمة السوقية للشركات العاملة في قطاع الضيافة في السنوات الخمس الماضية, حيث توصلت الدراسة أن عوائد السوق السلبية تحدث بعد الإعلانات عن الهجمات السيبرانية التي عانت منها شركات الضيافة. وتعتبر الاستثمارات الكافية في تكنولوجيا الأمن السيبراني وتدريب الموظفين ذات صلة بقطاع الضيافة للحد من المخاطر السيبرانية.

اما علي الجانب الآخر، فقد اتفقت بعض الدراسات السابقة علي وجود ردود فعل سلبية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم (Cheng&Walton,2019; Frank et al.,2019; Yang et al.,2020; Tosun,2021).

فهدفت دراسة Cheng & Walton (2019) إلي البحث عن تأثير وتوقيت الإفصاح عن خرق البيانات علي تقييمات وقرارات المستثمرين. وباستخدام عينة مكونة من (107) مستثمر غير محترف من 32 ولاية في الولايات المتحدة, توصلت الدراسة إلي أن وجود علاقة سلبية بين تقييم وقرارات المستثمرين والإفصاح عن خرق البيانات في وقت مبكر.

1- قطاع الضيافة: تشمل الفنادق والموتيلات بمختلف فئاتها والفنادق والمساكن بالعضوية وتشتمل العينة النهائية علي ست شركات ضيافة رائدة (مجموعة فنادق هواتشو، فنادق حياة، مجموعة فنادق إنتركونتيننتال، مجموعة فنادق ماندارين أورينتال، فنادق ومنتجعات ستاروود العالمية، وسيير لحلول الضيافة).

وعلي نفس السياق، هدفت دراسة Frank et al. (2019) إلي البحث في تأثير توكيد الطرف الثالث الطوعي علي برنامج إعداد تقارير إدارة مخاطر الأمن السيبراني علي جاذبية الاستثمار. وباستخدام عينة مكونة من 547 مستثمر غير محترف، توصلت إلي أن تضمين توكيد الإدارة فقط سيكون أكثر فعالية في حالة عدم تعرض الشركة لهجوم سيبراني لأن المستثمرين غير المحترفين لن يشككوا في مصداقية الإدارة. ايضاً، افترضت الدراسة أنه في حالة تعرض الشركة لهجوم سيبراني، فإن توكيد الطرف الثالث سيعزز جاذبية استثمارات الشركة. بشكل عام، فإن تقديم توكيد طرف ثالث بشأن تقارير إدارة مخاطر الأمن السيبراني سيكون له تأثير إيجابي علي جاذبية الاستثمار للشركة, لأنه يزيد من موثوقية الإدارة من وجهة نظر المستثمرين.

بالإضافة إلي ذلك, قدمت دراسة Yang et al., (2020) نموذجاً بحثياً لتصور وإدراك المستثمرين لإطار إعداد تقارير إدارة مخاطر الأمن السيبراني. وباستخدام عينة مكونة من 226 مستثمر غير محترف في الولايات المتحدة، توصلت الدراسة إلي أن جودة المعلومات والوعي بالأمن السيبراني سيكون لهما تأثير إيجابي علي الفوائد المدركة لبرنامج إدارة المخاطر وأن الثقة تتوسط هذه العلاقة وأن الفوائد المدركة للمستثمرين سيكون لها تأثير إيجابي علي قراراتهم في الاستثمار.

كما توصلت دراسة Tosun (2021) إلي وجود ردود فعل سلبية كبيرة علي أسعار الأسهم علي المدي القصير لاختراق بيانات الشركات، وتحديداً فإن الشركات التي تتعرض لتسريب معلومات سرية تعاني من انخفاض كبير في العوائد اللاحقة مقارنة بالشركات التي لا يتم اختراقها، وقد يكون للإفصاح عن الاختراقات الأمنية مرتبطة سلبياً بتغييرات أسعار الأسهم في خلال يومين من تاريخ الإفصاح. فأوضحت الدراسة أنه في المتوسط يكون للإفصاح عن اختراق أمن الشركات تأثير سلبي يبلغ حوالي 1% من القيمة السوقية للشركة في الأيام التي تلت الإفصاح, كما توصلت الدراسة إلي وجود اختلاف في تأثير هجمات الأمن السيبراني علي أسعار الأسهم المتداولة ويرجع ذلك إلي اختلاف نوعية المعلومات التي يتم الحصول عليها من تلك الهجمات فإذا كانت هذه الهجمات تمثل اختراق للمعلومات الخاصة بالعملاء فسيفقد العملاء ثقتهم في الشركة, ولكن إذا كانت الهجمات عبارة عن برامج خبيثة فإن التأثير المحتمل سيكون انخفاض التدفقات النقدية.

ويخلص الباحث إلي أنه رغم ندرة الدراسات السابقة إلي أن هناك اتفاق بين الدراسات علي أن هناك اهتماماً من جانب المستثمرين بتقرير إدارة مخاطر الأمن السيبراني، لأنه يمكن المستثمرين الجدد والحاليين علي تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات، مما يساهم في زيادة كفاءة وفعالية قرارات الاستثمار. ومع ذلك، فأن هناك تضارب بين نتائج الدراسات السابقة حيث وجدت بعض الدراسات ردود فعل إيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم

(Spanos&Angelis,2016; Arcuri et al.,2018; Amir et al.,2018; Berkman et al.,2018; Arcuri et al.,2020), بينما وجدت البعض الآخر وجود ردود فعل سلبية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم (Gordon et al., 2011; Morse et al., 2011; Pirounias et al., 2014;Hinz et al., 2015; Modi et al.,2015; Amir et al., 2018).

ومما سبق يمكن اشتقاق الفرض الرئيسي الأول (H_1) علي النحو التالي:

H_1 : يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية.

فيما يتعلق بأثر مستوي خبرة المستثمرين، قد اتفقت العديد من الدراسات (Bronwn et al., 2018; Espahodi et al., 2019; Pavlopouls et al., 2019; Akisik & Gal, 2020; Landau et al., 2020) علي أن قرار يتأثر بخصائص المستثمر نفسه مثل: خبرته، وهو ما يؤثر علي حكمه الشخصي، ومن ثم علي قراره. ويؤثر مستوي خبره المستثمر علي إدراكه وفهمه للمحتوي المعلوماتي لتقرير الإفصاح عن إدارة مخاطر الأمن السيبراني، مما قد يؤدي إلي التباين في قرار الاستثمار في أسهم نفس الشركة, حيث يختلف رد فعل المستثمر ذو الخبرة المرتفعة أكثر سرعة وتأثيراً من المستثمر ذو الخبرة المنخفضة.

ومما سبق يمكن اشتقاق الفرض الرئيسي الثاني (H_2) علي النحو التالي:

H_2: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر.

وفيما يتعلق بمستوي التأهيل العلمي للمستثمر، اشارت دراسة Bertrand & Schoar (2003) إلي إن حملة شهادة الماجستير المهني يكونوا أكثر تحفظاً مقارنة بالمديرين التنفيذيين الآخرين. وهذه النتائج تتفق مع دراسة Gul et al., (2013) التي توصلت إلي أن الخلفية التعليمية هي أحد الأسباب الجوهرية في اختلاف نتائج الأفراد، حيث قد تؤثر الخلفية التعليمية للأفراد علي معرفتهم وقيمهم ومدي تقبلهم للمخاطر, وعلي سبيل المثال: يميل المراجعين الخارجيين الذين يحملون شهادات دراسات عليا إلي أن يكونوا أكثر تحفظاً في تقاريرهم. كما توصلت دراسة Lan et al., (2018) باستخدام عينة تتكون من 9000 مستثمر في الصين، إلي وجود تأثير معنوي إيجابي لخصائص المستثمر مثل: مستوي تأهيله العلمي علي قرارته الاستثمارية. كما اشارت دراسة Hossain (2020) أهمية التعليم بالنسبة للمستثمرين حيث يجعلهم مؤهلين لاتخاذ القرارات بشأن استثماراتهم.

ومما سبق يمكن اشتقاق الفرض الرئيسي الثالث (H_3) علي النحو التالي:

H_3: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر.

وفيما يتعلق بمستوي التنمية المهنية للمستثمرين, توصلت دراسة (Gull et al.,2021;Wahyuni, 2022) إلي أهمية اختبار أثر السمات النوعية للمستثمر مثل: مستوي التنمية المهنية للمستثمر كمتغير معدل للعلاقة الرئيسية محل الدراسة. ولذلك، يتوقع الباحث وجود علاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني ومستوي التنمية المهنية للمستثمر.

ومما سبق يمكن اشتقاق الفرض الرئيسي الرابع (H_4) علي النحو التالي

H_4: يختلف التأثير الجوهري للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر.

8-3 الدراسة التجريبية للشركات الصغيرة والمتوسطة الحجم محل الدراسة

8-3-1 أهداف الدراسة التجريبية

تستهدف الدراسة التجريبية اختبار فروض البحث من خلال اختبار ما إذا كان هناك تأثير للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية. كما تستهدف الدراسة التجريبية ايضاً اختبار أثر كل من؛ مستوي خبرة المستثمر، ومستوي التأهيل العلمي للمستثمر، ومستوي التنمية المهنية للمستثمر كمتغيرات معدلة، علي العلاقة الأساسية محل الدراسة.

8-3-2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من المستثمرين المحترفين[1]، قياسًا على (Geiger and Kumar,2016; Kaplan et al,2014). وتتمثل عينة الدراسة في عينة انتقائية حكمية من مجتمع المستثمرين المؤسسين بالشركات الصغيرة والمتوسطة الحجم في البيئة المصرية، وقد تكونت العينة الحكمية من 253 مفردة. ويوضح الجدول التالي رقم (1) عدد الحالات الموزعة:

[1] المستثمرين المحترفين: وهما أمناء الاستثمار ومعاونيهم والمحللين الماليين المحترفين ومديري صناديق الاستثمار (Reimsbach el at., 2018; Hoang & Phang, 2021).

جدول 1: بيان بعدد الحالات الموزعة والردود عليها

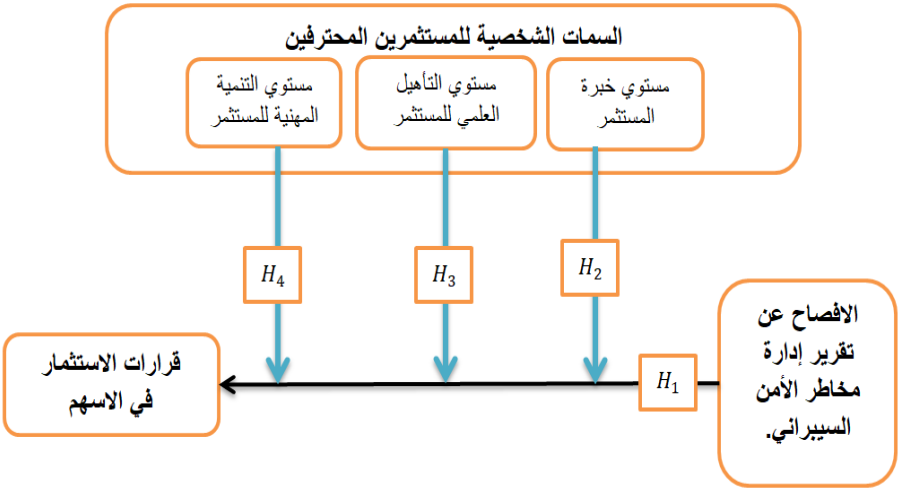
عدد الاستمارات الموزعة	عدد الردود المستلمة	نسبة الردود المستلمة	عدد الردود الصحيحة	نسبة الردود الصحيحة إلي الردود المستلمة
392	261	%66.6	204	%78.2

جدول 2: الحالات التجريبية الموزعة والردود عليها

الحالات التجريبية / البيان	الحالة التجريبية الأولي (القوائم المالية والايضاحات المتممة فقط)	الحالة التجريبية الثانية (القوائم المالية والايضاحات المتممة مرفق معها تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني)	الاجمالي
عدد الحالات الموزعة	186	206	392
عدد الحالات المستلمة	120	141	261
نسبة الاستجابة	%64.5	%68.5	%66.6
عدد الردود الصحيحة	85	119	204
نسبة الردود الصحيحة إلي المستلمة	%70.8	%84.4	%78.2

3-3-8 نموذج البحث وتوصيف وقياس متغيرات الدراسة

انطلاقاً من فروض البحث الرئيسية، فأن متغيرات الدراسة تتكون من متغير مستقل واحد، وهو الافصاح عن تقرير إدارة مخاطر الأمن السيبراني، ومتغير تابع واحد, وهو قرار الاستثمار في الأسهم، بالإضافة إلي ثلاث متغيرات معدلة وهما، مستوي خبرة المستثمر, ومستوي التأهيل العلمي للمستثمر، ومستوي التنمية المهنية للمستثمر، وذلك بغرض بيان أثر السمات النوعية للمستثمرين المحترفين علي العلاقة الرئيسية محل الدراسة. ويوضح الشكل التالي (3-1) نموذج البحث:



شكل 1: نموذج البحث – من إعداد الباحث

وفي ضوء هذا النموذج تم توصيف وقياس متغيرات الدراسة كما هو بالجدول (3) التالي:

جدول 3: توصيف وقياس متغيرات الدراسة

المتغير:	نوع المتغير:	توصيف المتغير:	قياس المتغير:
اولاً: المتغير المستقل:			
الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني	مستقل	تقرير يهدف إلي توصيل معلومات عن توكيدات الإدارة المتعلقة بتقييمها الفعال لإجراءات الرقابة المصممة لإدارة مخاطر الأمن السيبراني من خلال تقرير مرفق ضمن القوائم المالية. Yang et al., (2020)	إذا تم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يأخذ القيمة (1)، وفي حالة عدم الإفصاح يأخذ القيمة (صفر).
ثانياً: المتغير التابع:			
قرار الاستثمار في الأسهم	تابع	يقصد به استعداد المستثمرين للاستثمار في أسهم الشركة, واختيار بين بديلين أو أكثر من بين البدائل المتاحة وفق معيار العائد علي الاستثمار. شحاته (2014)	يتوقع سعر السهم للشركة في نهاية الفترة التالية واتخاذ قرار الاستثمار في الأسهم، قياسا علي (موسي،2018؛ محمد، 2020).
ثالثاً: المتغيرات المعدلة:			
مستوي خبرة المستثمر	معدل	هو المخزون المعرفي العملي الناتج عن ممارسة العمل المهني لصاحب المصلحة.	اذا كان لدي المستثمر خبرة أكبر من 5 سنوات يأخذ القيمة (1)، واذا كان غير ذلك يأخذ القيمة (0)، قياسا علي (موسي،2018؛ حامد،2019).
مستوي التأهيل العلمي للمستثمر	معدل	هو المخزون المعرفي العلمي الناتج عن التعليم الأكاديمي.	اذا كان المستثمر حاصلا علي دراسات عليا في مجال المحاسبة يأخذ القيمة (1), وغير ذلك يأخذ القيمة (0), قياسا علي (موسي،2018؛ Desimone & Rich, 2020).
مستوي التنمية المهنية للمستثمر	معدل	هو المخزون المعرفي الناتج عن التعليم المهني والشهادات المهنية الحاصل عليها.	اذا كان المستثمر حاصلا علي شهادات مهنية في مجال المحاسبة يأخذ القيمة (1)، وغير ذلك يأخذ القيمة (0)، قياسا علي (موسي،2018؛ Desimone & Rich, 2020).

8-3-4 أدوات وإجراءات الدراسة التجريبية

تعتمد الدراسة التجريبية علي الحالات التجريبية المدعومة بمجموعة من الاسئلة المرافقة لها لتجميع المشاهدات اللازمة، والمقابلات الشخصية، قياساً علي (الأباصيري,2018؛ Bartlett et al.,2016). وراعي الباحث عند تصميم الحالات التجريبية أن تكون كاملة وواضحة، ولذلك راعي إضافة وشرح بعض المصطلحات الفنية، والتي قد يصعب علي أفراد العينة إدراك المقصود منها.

ولإجراء الحالات التجريبية استرشد الباحث ببعض الدراسات السابقة، مثل: (Badawy,2021; Perols & Murthy, 2021) بهدف اختبار العلاقة محل الدراسة، حيث تم صياغة نموذج قياسي مقترح للتقرير عن إدارة مخاطر الأمن السيبراني، وتم تحديد المتغيرات المعدلة الثلاثة الذين من المفترض أن يؤثروا علي العلاقة محل الدراسة وهما: مستوي خبرة المستثمر، ومستوي التأهيل العلمي للمستثمر، ومستوي التنمية المهنية للمستثمر. وتم ترتيب الحالات التجريبية بما يخدم اختبار الفروض البحثية, وذلك علي النحو التالي:

القسم الأول: يشتمل علي البيانات الشخصية، والمتمثلة في الاسم, الوظيفة الحالية، المؤهلات الدراسية, الشهادات المهنية، وعدد سنوات الخبرة.

القسم الثاني: يتضمن مجموعة من المصطلحات الفنية ذات الصلة بنطاق البحث ومن أهمها: إدارة مخاطر الأمن السيبراني، الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، قرارات الاستثمار في الأسهم، والتي قد يصعب علي أفراد العينة إدراك المقصود منها.

القسم الثالث: يحتوي علي الحالة التجريبية الأولي: وتشتمل علي القوائم المالية الفعلية للشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية.

القسم الرابع: يحتوي علي الحالة التجريبية الثانية: وتشتمل علي القوائم المالية الفعلية للشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية, ومرفق معها تقرير للإفصاح عن إدارة مخاطر الأمن السيبراني.

ويرافق الحالات التجريبية مجموعة من الأسئلة للحصول علي اجابات مفردات العينة لمعرفة مدي استعدادهم للاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم. واعتمد الباحث بإجراء مجموعة من المقابلات الشخصية، والاتصالات الهاتفية مع بعض مفردات العينة لتوضيح هدف الدراسة، وللرد علي استفساراتهم.

وقد قام الباحث بتوزيع عدد 392 نسخة علي مفردات الدراسة عن طريق التسليم اليدوي ومواقع التواصل الاجتماعي (LINKED IN) والمقابلات الشخصية, بهدف الوصول إلي مجتمع الدراسة من المستثمرين. وبعد فترة تراوحت بين أسبوعين إلي 9 أسابيع استلم الباحث عدد 261 رد (بنسبة استجابة 66.6%)، وقد تم استبعاد عدد 57 رد اشتملوا علي إجابات متعارضة، وبذلك يكون عدد الردود الصحيحة 204 حالة، ثم تم تفريغ الردود علي برنامج EXCEL تمهيدا للتحليل الإحصائي واختبار الفروض من خلال برنامج SPSS.

8-3-5 التصميم التجريبي المستخدم والمعالجات والمقارنات التجريبية

لقد تم استخدام التصميم التجريبي (2x2x2) كما هو موضح في الجدول (4)، وذلك علي عينة من المستثمرين:

جدول 4: التصميم التجريبي المستخدم على عينة من المستثمرين

	مستوي خبرة المستثمر		مستوي التأهيل العلمي للمستثمر		مستوي التأهيل المهني للمستثمر	
	مرتفع	منخفض	مرتفع	منخفض	مرتفع	منخفض
الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.	(1) قرار الاستثمار	(3) قرار الاستثمار	(5) قرار الاستثمار	(7) قرار الاستثمار	(9) قرار الاستثمار	(11) قرار الاستثمار
عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.	(2) قرار الاستثمار	(4) قرار الاستثمار	(6) قرار الاستثمار	(8) قرار الاستثمار	(10) قرار الاستثمار	(12) قرار الاستثمار

وبناءً علي هذا التصميم, هناك (12) معالجة تجريبية كما يلي:

المعالجة رقم (1): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي خبرة المستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (2): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي خبرة المستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

المعالجة رقم (3): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي خبرة المستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (4): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي خبرة المستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

المعالجة رقم (5): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل العلمي للمستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (6): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل العلمي للمستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

المعالجة رقم (7): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل العلمي للمستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (8): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل العلمي للمستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

المعالجة رقم (9): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل المهني للمستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (10): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل المهني للمستثمر مرتفع/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

المعالجة رقم (11): الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل المهني للمستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير التقرير علي قرار الاستثمار.

المعالجة رقم (12): عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني/ في حالة مستوي التأهيل المهني للمستثمر منخفض/ ويطلب من فئات العينة تحديد مدي تأُثير عدم وجود التقرير علي قرار الاستثمار.

ولاختبار فروض البحث تم إجراء المقارنات التالية بين المعالجات التجريبية:

المقارنة رقم (1): (1+3+5+7+9+11) X (2+4+6+8+10+12), وذلك لاختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية، ومن ثم اختبار الفرض الرئيسي الأول (H_1).

المقارنة رقم (2): (1 X 2) X (3 X 4), وذلك لاختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر, ومن ثم اختبار الفرض الرئيسي الثاني (H_2).

المقارنة رقم (3): (5 X 6) X (7 X 8), وذلك لاختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي المستثمر, ومن ثم اختبار الفرض الرئيسي الثالث (H_3).

المقارنة رقم (4): (9 X 10) X (11 X 12), وذلك لاختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية المستثمر، ومن ثم اختبار الفرض الرئيسي الرابع (H_4).

8-3-6 الأساليب الإحصائية المستخدمة ونتائج اختبار فروض البحث

وفقاً لطبيعة البيانات ومنهجية الدراسة، اعتمد الباحث علي عدد من الأساليب الإحصائية المختلفة المتعلقة ببرنامج SPSS لتحليل البيانات. وقام الباحث باستخدام الجداول الإلكترونية الخاصة ببرنامج Microsoft Excel من أجل تفريغ ردود المشاركين في الدراسة التجريبية, ثم تم إجراء الاختبارات

الإحصائية باستخدام برنامج التحليل الإحصائي SPSS. وقد استخدم الباحث الاختبارات الإحصائية التي تتفق مع طبيعة بيانات الدراسة التجريبية وفروض البحث, كالتالي:

- **الأساليب الإحصائية المتعلقة بقياس الصدق والثبات:**

تم اجراء اختبار كرونباخ ألفا Cronbach`s Alpha لقياس الصدق والثبات، حيث يقيس هذا الاختبار مدي ثبات إجابات أفراد العينة علي الأسئلة المقدمة لهم, واختبار مدي الموثوقية في استجاباتهم، ومدي صلاحية بيانات الدراسة للتحليل الإحصائي لمعرفة مدي إمكانية تعميم النتائج، التي تم الحصول عليها من العينة، علي مجتمع الدراسة. وتقبل قيمة المعامل إذا تجاوزت 50% وهو ما تحقق في هذا البحث، حيث أظهرت النتائج أن قيمة كرونباخ ألفا (.732) وهو ما يمثل مستوي جيدا من الصدق والثبات.

- **تحديد نوع توزيع المجتمع Test of Normality:**

لتحديد نوع توزيع المجتمع, الذي تم سحب عينة الدراسة منه, وذلك من أجل تحديد ما إذا كان سيتم استخدام الاختبارات المعلمية Parametric tests أو الاختبارات اللامعلمية Non parametric tests، تم اجراء اختبار كلوموجروف – سيمرنوف Kolomgrov–Smirrnov، لمعرفة ما إذا كان هذا التوزيع يتبع التوزيع الطبيعي أم لا (Peck & Devor,2012). وتوضح دراسة (Abdollahyan,2020) أنه إذا أظهرت نتائج هذا الاختبار أن قيمة P–value أقل من مستوي المعنوية (5%) يتم رفض فرض العدم (القائل بأن المجتمع الذي سحبت منه عينة البحث يتبع التوزيع الطبيعي). وأظهرت نتائج هذا الاختبار أن قيمة P–Value مساوية (٠.٠٠٠) لجميع متغيرات البحث محل الدراسة، أي أقل من مستوي المعنوية (5%) مما يعني رفض فرض العدم (القائل بأن المجتمع الذي سحبت منه عينة البحث يتبع التوزيع الطبيعي) وقبول الفرض البديل (القائل بأن المجتمع الذي سحبت منه عينة البحث لا يتبع التوزيع الطبيعي). وبناء علي ذلك تم الاعتماد علي الاختبارات اللامعلمية لاختبار فروض البحث.

8-4 تحليل نتائج البحث

فيما يلي يعرض الباحث نتائج اختبار فروض البحث الرئيسية والفرعية, كل علي حده:

- **نتائج اختبار الفرض الرئيسي الاول (H_1):**

استهدف الفرض الأول اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية. وقد استخدم الباحث في هذا الشأن اختبار مان ويتني اللامعلمي لعينتين مستقلتين لإجراء المقارنات الثنائية وتحديد مدي الاختلاف بين وسيطي عينتين مستقلتين. وقد تم تحويل الفرض البديل إلي صورة فرض العدم كما يلي:

H_0: لا يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية.

وتم صياغة هذا الفرض إحصائيا كما يلي (Two tail test):

وسيط ردود العينة الأولي (الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني) يساوي وسيط ردود العينة الثانية (عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني).

$$\mu_2 = \mu_1 : H_0$$

مقابل الفرض البديل:

وسيط ردود العينة الأولي (الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني) لا يساوي وسيط ردود العينة الثانية (عدم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني).

$$\mu_2 \neq \mu_1 : H_1$$

ويوضح الجدول التالي الاختبار الإحصائي لهذا الفرض:

جدول 5: نتيجة الاختبار الإحصائي للفرض (H_1)

اسم الاختبار الاحصائي	P-Value
Mann-Whitney U	690.00
Asymp. Sig. (2-tailed)	.000

ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P−value < 5%, ويتم قبول فرض العدم إذا كانت قيمة P−Value > 5%. وبالنظر لنتيجة اختبار مان ويتني كانت قيمة P−Value = (0.000) أصغر من 5% وبالتالي يتم رفض فرض العدم وقبول الفرض البديل (H_1). ومن ثم يمكن القول بأنه يوجد تأثير إيجابي معنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية.

- **نتائج اختبار الفرض الرئيسي الثاني (H_2):**

استهدف الفرض الثاني اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر. وقد استخدم الباحث في هذا الشأن اختبار مان ويتني اللامعلمي لعينتين مستقلتين لإجراء المقارنات الثنائية وتحديد مدي الاختلاف بين وسيطي عينتين مستقلتين. وقد تم تحويل الفرض البديل إلي صورة فرض العدم كما يلي:

H_0: لا يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر.

وتم صياغة هذا الفرض إحصائيا كما يلي (Two tail test):

وسيط ردود العينة الأولي يساوي وسيط ردود العينة الثانية.

$$\mu_2 = \mu_1 : H_0$$

مقابل الفرض البديل:

وسيط ردود العينة الأولي لا يساوي وسيط ردود العينة الثانية.

$$\mu_2 \neq \mu_1 : H_2$$

ويوضح الجدول التالي الاختبار الإحصائي لهذا الفرض:

جدول 6: نتيجة الاختبار الإحصائي للفرض (H_2):

اسم الاختبار الاحصائي	P-Value
Mann-Whitney U	308.500
Asymp. Sig. (2-tailed)	.020

ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P−value < 5%, ويتم قبول فرض العدم إذا كانت قيمة P−Value > 5%. وبالنظر لنتيجة اختبار مان ويتني كانت قيمة P−Value = (0.020) أصغر من 5% وبالتالي يتم رفض فرض العدم وقبول الفرض البديل (H_2). ومن ثم يمكن القول بأنه يوجد تأثير إيجابي معنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي خبرة المستثمر.

- **نتائج اختبار الفرض الرئيسي الثالث (H_3):**

استهدف الفرض الثالث اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر. وقد استخدم الباحث في هذا الشأن اختبار مان ويتني اللامعلمي لعينتين مستقلتين لإجراء المقارنات الثنائية وتحديد مدي الاختلاف بين وسيطي عينتين مستقلتين. وقد تم تحويل الفرض البديل إلي صورة فرض العدم كما يلي:

H_0: لا يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر.

وتم صياغة هذا الفرض إحصائيا كما يلي (Two tail test):

وسيط ردود العينة الأولي يساوي وسيط ردود العينة الثانية.

$$\mu_2 = \mu_1 : H_0$$

مقابل الفرض البديل:

وسيط ردود العينة الأولي لا يساوي وسيط ردود العينة الثانية.

$$\mu_2 \neq \mu_1 : H_3$$

ويوضح الجدول التالي الاختبار الإحصائي لهذا الفرض:

جدول 7: نتيجة الاختبار الإحصائي للفرض (H_3):

اسم الاختبار الاحصائي	P-Value
Mann-Whitney U	223.500
Asymp. Sig. (2-tailed)	.006

ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P−value < 5%, ويتم قبول فرض العدم إذا كانت قيمة P−Value > 5%. وبالنظر لنتيجة اختبار مان ويتني كانت قيمة P−Value = (0.006) أصغر من 5% وبالتالي يتم رفض فرض العدم وقبول الفرض البديل ($_3$). ومن ثم يمكن القول بأنه يوجد تأثير إيجابي معنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر.

- **نتائج اختبار الفرض الرئيسي الرابع (H_4):**

استهدف الفرض الرابع اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر. وقد استخدم الباحث في هذا الشأن اختبار مان ويتني اللامعلمي لعينتين مستقلتين لإجراء المقارنات الثنائية وتحديد مدي الاختلاف بين وسيطي عينتين مستقلتين. وقد تم تحويل الفرض البديل إلي صورة فرض العدم كما يلي:

H_0: لا يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر.

وتم صياغة هذا الفرض إحصائيا كما يلي (Two tail test):

وسيط ردود العينة الأولي يساوي وسيط ردود العينة الثانية.

$$\mu_2 = \mu_1 : H_0$$

مقابل الفرض البديل:

وسيط ردود العينة الأولي لا يساوي وسيط ردود العينة الثانية.

$$\mu_2 \neq \mu_1 : H_3$$

ويوضح الجدول التالي الاختبار الإحصائي لهذا الفرض:

جدول 8: نتيجة الاختبار الإحصائي للفرض (H_4):

اسم الاختبار الاحصائي	P-Value
Mann-Whitney U	313.500
Asymp. Sig. (2-tailed)	.062

ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P−value < 5%، ويتم قبول فرض العدم إذا كانت قيمة P−Value > 5%. وبالنظر لنتيجة اختبار مان ويتني كانت قيمة P−Value = (0.062) أصغر من 5% وبالتالي يتم قبول فرض العدم ورفض الفرض البديل (H_4). ومن ثم يمكن القول بأنه لا يوجد تأثير إيجابي معنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر.

وتتفق هذه النتيجة مع بعض الدراسات (Ohman et al.,2012;Sofiyanti& Rahmawati, 2022) بينما تختلف مع البعض الآخر (Rena et al, 2016; Hoang & Phang, 2021)، ويمكن أن يرجع ذلك لوجود تأييد من قبل المستثمرين سواء كانوا حاصلين علي شهادات مهنية أم لا، علي أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، حيث يؤثر ذلك الإفصاح معنوياً وإيجابياً علي قرارات الاستثمار.

8-4-1 خلاصة نتائج اختبار فروض البحث

يمكن عرض خلاصة نتائج اختبار فروض البحث كالتالي:

فروض البحث:	صيغة الفرض البديل:	نتيجة اختبار الفرض:
H_1	يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني معنوياً علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية.	تم قبول الفرض.
H_2	يختلف التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي خبرة المستثمر.	تم قبول الفرض.
H_3	يختلف التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر.	تم قبول الفرض.
H_4	يختلف التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في الشركات الصغيرة والمتوسطة الحجم المقيدة بالبورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر.	تم رفض الفرض.

8-5 النتائج والتوصيات والدراسات المستقبلية

ارتكازاً على عرض وتحليل المحاور الرئيسية التي تحقق أهداف البحث، ومن واقع الدراسة التجريبية للشركات الصغيرة والمتوسطة الحجم التي مثلت العينة، يمكن للباحث استخلاص أهم النتائج وتقديم التوصيات والدراسات المستقبلية على النحو التالي:

8-5-1 نتائج الدراسة

- **كشفت الدراسة النظرية عن مجموعة من النتائج أهمها ما يلي:**

- اتفقت معظم الدراسات السابقة علي إن إدارة مخاطر الأمن السيبراني يقصد بها قيام الشركات بتبني برنامج محدد ومناسب يمكنها من تنفيذ وتشغيل ضوابط رقابية تساعدها علي حماية أنظمتها وأصولها المعلوماتية. ولتحسين عملية إدارة هذه المخاطر، تحتاج الشركات إلي تنمية الوعي، والاهتمام بتضمين الممارسات الجيدة في مجال إدارة مخاطر الأمن السيبراني, واعتماد منهجية أكثر مرونة للاستجابة للتهديدات السيبرانية الجديدة والمتطورة، وذلك من أجل تعظيم الفوائد التي تعود علي الشركة من الإدارة الفعالة لمخاطر الأمن السيبراني.
- وتوصل البحث في شقه النظري, إلي أنه علي الرغم من أن هناك العديد من جهات وضع المعايير والجهات الرقابية والهيئات المنظمة في الدول المختلفة، اهتمت بتطوير وتنظيم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني من خلال إصدار العديد من الإرشادات المهنية, إلا أنه في مصر، وعلي الرغم من الاهتمام بإصدار القوانين المنظمة للأمن السيبراني, إلا أنه لم يتم إصدار إرشادات أو معايير منظمة لعملية إعداد والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في مصر.

- وتوصل البحث إلي أنه علي الرغم من تضارب نتائج بعض الدراسات السابقة، حيث توصلت بعض الدراسات إلي وجود علاقة إيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في الأسهم، بينما توصل البعض الآخر أن هناك علاقة سلبية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات الاستثمار في الأسهم, إلي أن الباحث توصل أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يرسل إشارات إيجابية عن الشركات للمستثمرين وغيرهم من أصحاب المصالح, حول مدي اهتمام الشركة بإدارة مخاطر الأمن السيبراني. مما قد يساعد المستثمرين في تحسين قرارات الاستثمار.
- تسهم تقارير الإفصاح عن إدارة مخاطر الأمن السيبراني بشكل فعال في القضاء على نقص الشفافية وعدم تماثل المعلومات، مما يؤثر بشكل مباشر على دقة وسلامة القرارات التي يتم اتخاذها للشركة وعلى مستخدمي القوائم والتقارير المالية نظراً لزيادة مستوى جودة المعلومات المقدمة لهم, ومما يمكن المستثمرين من تقييم مدي كفاءة الشركة في الحفاظ علي أمن المعلومات وتقليل اي اختراقات أو أحداث مستقبلية ممكن تحدث في المستقبل.
- أكدت معظم الدراسات على أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني له العديد من الآثار الإيجابية حيث أنه يسهم في تعزيز إدراك أصحاب المصالح لجودة المعلومات المقدمة.
- بالإضافة إلى ذلك، يمكن تقرير الإفصاح عن مخاطر الأمن السيبراني مساعدة الشركات الصغيرة والمتوسطة الحجم في تحسين صورة وسمعة الشركة ومن ثم أسعار الأسهم مما يحسن من مساعدة المستثمرين على اتخاذ القرارات المتعلقة بالاستثمار مما يعمل علي تحسين الأداء المالي للشركة.
- كما توصل الباحث أن قرارات المستثمرين تعتمد في كثير من الأحيان علي بعض الخصائص الشخصية المتعلقة بالمستثمر نفسه, حيث أن خبرة المستثمر ومستوي تأهيله العلمي ومستوي تأهيله المهني يؤثر علي تحسين إدراكه وفهمه لمحتوي تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني, مما يؤثر علي تحسين جودة القرارات المتخذة.

- **وقد كشفت الدراسة التجريبية عن مجموعة من النتائج أهمها ما يلي:**

- كشفت نتائج التحليل الوصفي لتقرير الإفصاح عن إدارة مخاطر الأمن السيبراني عن ضعف التزام معظم الشركات الصغيرة والمتوسطة الحجم محل الدراسة بالإفصاح عن تقرير مخاطر الأمن السيبراني رغم المميزات التي يقدمها تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني من تعزيز جودة المعلومات والبيانات في القوائم المالية.

- تبين من نتائج التحليل الوصفي للخصائص الشخصية للمستثمرين إلي أنه في كثير من الأحيان تؤثر سماتهم وخصائصهم الشخصية علي جودة قراراتهم في الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم محل الدراسة.
- أكدت نتائج الدراسة التجريبية على وجود علاقة إيجابية معنوية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية، حيث كانت قيمة P–Value = (0.000) أصغر من 5%، وبالتالي تم قبول الفرض الرئيسي الأول (H_1).
- كما أكدت نتائج الدراسة التجريبية علي وجود علاقة إيجابية معنوية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي خبرة المستثمر, حيث كانت قيمة P–Value = (0.020) أصغر من 5%، وبالتالي تم قبول الفرض الرئيسي الثاني (H_2).
- وأكدت نتائج الدراسة التجريبية علي وجود علاقة إيجابية معنوية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي التأهيل العلمي للمستثمر، حيث كانت قيمة P–Value = (0.006) أصغر من 5%، وبالتالي تم قبول الفرض الرئيسي الثالث (H_3).
- وتوصلت ايضاً نتائج الدراسة التجريبية إلي عدم وجود علاقة معنوية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرار الاستثمار في أسهم الشركات الصغيرة والمتوسطة الحجم المقيدة في البورصة المصرية باختلاف مستوي التنمية المهنية للمستثمر, حيث كانت قيمة P–Value = (0.062) أكبر من 5%، وبالتالي تم رفض الفرض الرئيسي الرابع (H_4).
- كما أكدت نتائج الدراسة التجريبية على أن الإفصاح عن تقرير مخاطر إدارة الأمن السيبراني يسهم في تحسين مستوي جودة المعلومات المقدمة وزيادة الثقة في الشركات وزيادة القدرة علي اتخاذ قرارات ذات كفاءة وفعالية.

8-5-2 توصيات الدراسة

في ضوء نتائج الدراسة النظرية والتجريبية وتمشياً مع التطورات الدولية المعاصرة وإرتقاءاً بمهنة المحاسبة والمراجعة وتطويراً لقطاع الشركات الصغيرة والمتوسطة الحجم لما لها من أهمية في الاقتصاد القومي، يمكن للباحث تقديم مجموعة من التوصيات أهمها ما يلي:

- ضرورة زيادة الوعي بأهمية التقرير للإفصاح عن إدارة مخاطر الأمن السيبراني، من خلال المؤتمرات والمقالات العلمية.

- ضرورة قيام الجهات الرقابية والمنظمة المصرية بإصدار الإرشادات والمعايير اللازمة عن محتوي تقرير إدارة مخاطر الأمن السيبراني.
- ضرورة اهتمام الهيئة العامة للرقابة المالية المصرية بتوجيه وزيادة وعي الشركات عن أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، من خلال نشر ثقافة الإفصاح عن هذه المعلومات في تقارير الشركات.
- تحفيز الشركات متناهية الصغر والصغيرة والمتوسطة الحجم نحو أهمية تبنى الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني مما يعمل علي تحسين سمعة الشركة وزيادة الاستثمارات بها.
- يجب علي الباحثين إجراء المزيد من الأبحاث في مجال الإفصاح عن إدارة مخاطر الأمن السيبراني، ودراسة أثره علي قرارات المستثمرين.
- ضرورة تفعيل تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات الصغيرة والمتوسطة الحجم وفقاً لأسس قانونية وفنية ومالية قوية، بما يسهم في تطوير أساليب الافصاح والشفافية للمعلومات والقوائم والتقارير المالية، ومن ثم تعزيز كفاءة وفاعلية الأسواق بوجه خاص الاقتصاد القومي بوجه عام.
- عقد الندوات العلمية والبرامج التدريبية المتخصصة بشأن المحاسبة والمراجعة والتعريف بأهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، لتأهيل جيل جديد من المحاسبين والمراجعين وأصحاب الشركات متناهية الصغر والصغيرة والمتوسطة الحجم يواكب التطورات والتغيرات المتلاحقة بسوق الأعمال.

8-5-3 الدراسات المستقبلية التي ترتبط بمجالات البحث

يمكن للباحثين والمهتمين اجراء مزيد من الدراسات والبحوث التي ترتبط بتطبيق أنظمة المحاسبة الذكية عبر الهاتف في كل من المجالات التالية:

- أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي إدراك المستثمرين الجودة الحقيقية والمتوقعة لجودة التقارير: مع دراسة تجريبية بالشركات الصغيرة والمتوسطة الحجم.
- أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي سمعة الشركة والأداء المالي.
- قياس أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على دقة توقعات المحللين الماليين: مع دراسة تطبيقية بالشركات المقيدة بالبورصة المصرية.
- مدخل مقترح لتفعيل أنشطة المراجعة الداخلية بشأن تقرير الإفصاح عن إدارة مخاطر الأمن السيبراني: مع دراسة ميدانية بالشركات الصغيرة والمتوسطة الحجم.

المراجع

أولاً: المراجع باللغة العربية

الاستراتيجية الوطنية للأمن السيبراني، (2017-2018) ، المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء، جمهورية مصر العربية, ص ص 1- 19.

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

حامد، سحر سعيد. (2019). أثر الإسناد والتوقيت والوضع الوظيفي للمراجعة الداخلية علي قرار المراجع الخارجي بشأن مدي اعتماده علي وظيفة المراجعة الداخلية – دراسة تجريبية. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة دمنهور.

حسن، امتثال محمد حسن، وأحمد، محمد علي محمد. (2000). مبادئ الاستدلال الإحصائي. قسم الإحصاء والرياضة والتأمين، كلية التجارة – جامعة الإسكندرية.

موسي، سعاد زغلول عبده. (2018). أثر توكيد المراجع الخارجي علي تقارير الأعمال المتكاملة علي قراري الاستثمار ومنح الائتمان: دراسة تجريبية. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.

ثانياً: المراجع باللغة الأجنبية

American Institute of Certified Public Accountants (AICPA) (2018). Cyber security risk management reporting fact sheet. (Accessed 12 November 2020). Available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/ assurance-advisoryservices/downloadabledocuments/cybersecurity-factsheet.pdf.

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

American Institute of Certified Public Accountants (AICPA), 2018, Illustrative cybersecurity risk management report, , United States, PP 1 29.

American Institute of Certified Public Accountants (AICPA). (2017a). SOC for Cybersecurity: A Backgrounder. AICPA, 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.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. **Corporate Ownership & Control**, 15(2), 70-83.

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. **Journal of Hospitality and Tourism Technology**, 11(2), 277-290.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. **Decision Support Systems**, 147,113580.

Badawy, H., 2021, The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study, **Alexandria Journal of Accounting Research**, 3 (5): 1-56.

Bao Ngo, T. N., & Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. **Interdisciplinary Description of Complex Systems**: **INDECS**, 19(3), 375-390.

Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. **Journal of Accounting and Public Policy**, 106998.

Berkman, H., Jona, J., Lee, G., and Soderstorm, N., 2018, Cybersecurity Awareness and Market Valuations, **Journal of Accounting and Public Policy**, 37 :508-526.

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). Equifax says cyberattack may have affected 143 million in the US. The New York Times, A1. Bourdon, B. (2019), "The adorable mistakes executives continue to make after a data breach," **Harvard Business Review**, **Press**, **Boston**.

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.

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. **German Law Journal**, 21(6), 1149-1179.

Chartered Professional Accountants Of Canada (CPA Canada).(2018). Reporting Alert CORPORATE REPORTING: Cyber Security: Establishing A Risk Management Program And Continuing To Reassess Disclosure Practices, CPA Canada.

Chartered Professional Accountants Of Canada (CPA Canada).(2018). Cyber Security Risks and Incidents — Reassessing Your Disclosure Practices, CPA Canada.

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.

CPA Canada. 2017. Cyber security risks and incidents: Reassessing your disclosure practices.

Craigen, D., Diakun, N. and Purse, R., 2014, Defining Cybersecurity, **Technology Innovation Management Review**, 4 (10): 13-21.

CSA (Canadian Securities Administrator), 2017, Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents.

Eaton, T., Grenier, J. and Layman, D., (2019), Accounting and Cybersecurity Risk Management, **American Accounting Association**, 13 (2): 1-9.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. **Journal of Accounting and Public Policy**, 37(6), 564-585.

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.

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

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: **An International Journal**, 25/2, 223–240.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. **Journal of Cybersecurity**, 1(1), 3-17.

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** (**WEIS**) .1:37

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance. **Journal of Information Systems**, 35(2), 37-60.

Heller, M. (2017). "Cyber attacks can cause major stock drops." CFO.com April 12, 2017.

Heroux, S. and Anne, F., (2020), Cybersecurity Disclosure by the Companies on the S&PTSX 60 Index, **Accounting Perspectives**/**Perspectives Compatibles**, 19 (2): 73-100.

Hilary, G., Segal, B., and Zhang, M., 2016, Cyber-risk disclosure: Who cares? Research paper, https://**papers**.**ssrn**.**com**.

Jr, S. U. & Arnold ,C.(2019). Cybersecurity Is Critical for all Organizations– Large and Small, IFAC, Available at : https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small.

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**.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation,and the impact of successful cyberattacks on target firms. **Journal of Financial Economics**.

Kamiya, S., Kang, J., Kim, J., and Stulz, R., (2021), Risk management, firm reputation, and the impact of successful cyberattacks on target firms, **Journal of Financial Economics**, 139: 719–749.

Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security: **a review**. **Journal of King Saud University-Computer and Information Sciences**.

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

Khari, M., Shrivastava, G., Gupta, S., & Gupta, R. (2017). Role of Cyber Security in Today's Scenario. **In Detecting and Mitigating Robotic Cyber Security Risks**, **IGI Global** ,pp. 177-191.

KPMG. 2018. Growing pains: 2018 U.S. CEO outlook. Available at: https://assets.kpmg/content/dam/kpmg/us/pdf/2018/05/kpmg-ceooutlook.2018.pdf.

Krus, C. M. (2012), "Who is listening? The SEC emphasizes importance of cybersecurity disclosure", **Journal of Investment Compliance**, 13 (1) , 30-32.

Lan, Q., Xiong, Q., He, L. and Ma, C., 2018, Individual investment decision behaviors based on demographic characteristics: Case from China, **PLOS ONE**, 13 (8): 1-16.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. **Business Horizons**, 64, 659-671.

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

Li, H., No, W. G., Cheong, A., & Halterman, C. K.(2021). Data analytics in cybersecurity assurance: should data analytics be an integral part of cybersecurity assurance? Available at: https://zicklin.baruch.cuny.edu/wp-content/uploads/sites/10/2019/12/Data-Analytics-in-Cybersecurity-Assurance-1.pdf.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. **Energy Reports**. Volume 7, Pages 8176-8186.

Lutfi, L., (2010), The Relationship Between Demographic Factors and Investment Decision in Surabaya, **Journal of Economics**, **Business and Accountancy Ventura**, 13 (3): 213-224.

Masoud, N., & Al-Utaibi, G. (2022). The Determinants of Cybersecurity Risk Disclosure in Firms' Financial Reporting: Empirical Evidence. **Research in Economics**.

Miazee, M. & Hasan, M., (2014), Fundamentals Knowledge of Investment in Capital Market- A Study from Dhaka Stock Exchange, **Research Journal of Finance & Accounting**, 5 (24).

Mishra, K. & Medtilda, M., (2015), A Study on Impact of Investment Experience, Gender, & Level of Education on Overconfidence & Self – Attribution Bias, **IIMB management review**, 27 (3): 228-239.

Mohan, V., Simon, D., Rosenfeld, R., and Brown, M. (2021), "SEC increasingly turns focus toward strength of cyber risk disclosures", available at: https://corpgov.law.harvard.edu/2021/07/25/sec-increasingly-turns-focus-towardstrength-of-cyber-risk-disclosures/ (accessed 25 November 2021).

Moshaigeh, A., Dickins, D. and Higgs, J., 2019, Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution?, **The CPA Journal**, 89 (6): 36-41.

Navarro, P., & Sutton, S.G.(2021), Investors' Judgment and Decisions after a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance. Available at SSRN: https://ssrn.com/abstract=3817763 or http://dx.doi.org/ 10.2139/ ssrn. 381 7763.

No, W. and Vasarhelyi, M., 2017, Cybersecurity and Continuous Assurance, **Journal of Emerging Technologies in Accounting**, 14 (1): 1-12.

Obamuyi T., 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.

Perols, R. and Murthy, U., (2021), The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions, Auditing: **A Journal of Practice & Theory**, 40 (1): 73-89.

Perols, R. R. (2019). Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions (Doctoral dissertation, University of South Florida). Retrieved from https://scholarcommons.usf.edu/etd/8401.

PricewaterhouseCoopers (PWC). (2016). Turnaround and transformation in cyber security: Retail and consumer key findings from The Global State of Information Security Survey 2016. Available at: https://www. pwc.ru/ en/retail- onsumer/publications/assets/2016_ gsiss_rc.pdf.

PricewaterhouseCoopers (PwC). (2019). CEOs' curbed confidence spells caution. Available at: https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo survey.pdf.

Public Company Accounting Oversight Board (PCAOB). (2019). Cybersecurity: Where we are; what more can be done? A call for auditors to lean in. Available at: https://pcaobus.org/News/Speech/Pages/hamm-cybersecu-rity-wherewe-are-what-more-can-be-done.aspx.

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. **Cluster Computing**, 23(3), 1827-1843.

SEC. (2011). Division of Corporation Finance. CF disclosure guidance: Topic No.2,Cybersecurity.https://www.sec.gov/divisions/corpfin/guidance/cfg uidance topic2 .htm

SEC. (2018). 17 CFR Parts 229 and 249. [Release Nos. 33-10459; 34-82746]. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/ rules/interp/2018/33-10459.pdf.

Securities and Exchange Commission (SEC). (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures Release Nos. 33-10459; 34-82746. Available at: https://www.sec.gov/rules /interp/ 2018/33-10459.pdf.

Securities and Exchanges Commission – SEC (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. (February 2018) Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accessed December 19, 2018).

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

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

Tysiac, k.(2020). Cybersecurity provides opportunities for auditors to serve, Available at: https://www.journalofaccountancy.com/ news/2020/oct/ cybe rsecurity-opportunities-for-auditors.html.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. **Risk Management**, 22(4), 239-309.

Vekez, P. N. (2019). Three Studies on Cybersecurity Disclosure and Assurance (Doctoral dissertation, University of Central Florida). Electronic Theses and Dissertations, 2004-2019. 6541. https://stars. library. ucf. edu/ etd/ 6541.

Walton, S., Wheeler, P., Zhang, Y., & Zhao, X. (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future DirectionsAn Integrative Review and Analysis of Cybersecurity Research. **Journal of Information Systems**, Vol. 35, No. 1, pp. 155–186.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. **International Journal of Law**, **Crime and Justice**, 62, 100415.

Yang, L., Lau, L. and Jan, 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

في إطار قيام الباحث بإعداد بحث, والذي يتعلق بموضوع:

أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في الشركات الصغيرة والمتوسطة الحجم

دراسة تجريبية علي الشركات المقيدة بالبورصة المصرية

مقدم لسيادتكم القوائم المالية وتقرير إدارة مخاطر الأمن السيبراني للشركة (س) ومرفق معها قائمة استقصاء, لذا نرجو من سيادتكم التكرم بالإجابة علي بيانات هذه القائمة بكل وضوح، حيث يمثل ذلك جزء من متطلبات تحقيق الهدف من البحث، وتعد مشاركتكم هامة جداً لأغراض الدراسة.

ويقدر الباحث مسبقاً حسن تعاونكم ومساهمتكم الفعالة في إثراء المعرفة المحاسبية، ويأمل في تعاونكم بإبداء رأيكم في الأسئلة المرافقة للحالات الافتراضية. ويؤكد الباحث علي أن جميع ردودكم سوف تحظي بالسرية التامة، ولن تستخدم إلا لغرض البحث العلمي فقط.

وشكراً مقدماً علي حسن تعاونكم

وتفضلوا بقبول فائق الاحترام والتقدير..

الباحث

د/ كريم محمد حافظ توفيق القاضي

مدرس المحاسبة والمراجعة بقسم نظم معلومات الأعمال

المعهد العالي للسياحة والفنادق والحاسب الآلّي

السيوف – الإسكندرية

dr.karim.hafez.elkady@gmail.com

اولاً: البيانات العامة

الاسم: .....

الوظيفة الحالية: .....

المؤهل العلمي: .....

الشهادات المهنية: .....

عدد سنوات الخبرة: .....

ثانياً: أهم المصطلحات الفنية ذات الصلة بالبحث

- **الأمن السيبراني (Cybersecurity):** هو مجموعة من التقنيات والعمليات التي يتم تصميمها لحماية أجهزة الكمبيوتر والشبكات وقواعد البيانات والتطبيقات بما تحتويه من بيانات وما تقدمه من خدمات, من الهجمات الالكترونية والوصول غير المصرح به, والتغيير، أو التعطيل، أو سوء استخدام، أو استغلال غير مشروع.
- **مخاطر الأمن السيبراني:** من أكبر المخاطر التي تواجهها الشركات، حيث يمكن لمخاطر الأمن السيبراني أن تؤدي إلي ارتفاع التكاليف والتأثير السلبي علي عوائد الشركات, والإضرار بقدرة الشركة علي الابتكار واكتساب العملاء والحفاظ عليهم. كما أن الهجمات الإلكترونية مكلفة ولها تأثير واضح علي المركز المالي للشركات.
- **إدارة مخاطر الأمن السيبراني:** أنها مجموعة من السياسات والعمليات والاجراءات الرقابية المصممة لحماية المعلومات والأنظمة الالكترونية من الحوادث الأمنية التي تعرض أمن الشركة السيبراني لمخاطر عدم تحقيق أهدافه، كما تساعد تلك الإجراءات علي اكتشاف الهجمات الأمنية والاستجابة لها والتخفيف من آثارها، وسرعة التخلص من الآثار السلبية الناتجة عن الهجمات التي لا يمكن منعها.
- **الافصاح عن تقرير إدارة مخاطر الأمن السيبراني:** تقرير يهدف إلي توصيل معلومات عن توكيدات الإدارة المتعلقة بتقييمها الفعال لإجراءات الرقابة المصممة لإدارة مخاطر الأمن السيبراني من خلال تقرير مرفق ضمن القوائم المالية.

ثالثاً: الحالات التجريبية

الحالة التجريبية الأولي

شركة "س" هي شركة مساهمة مصرية تأسست في 2 فبراير 2008 طبقاً لأحكام القانون رقم 159 لسنة 1981، وهي شركة مقيدة بالبورصة المصرية, وتقوم بإعداد قوائمها المالية وفقاً لمعايير المحاسبة المصرية والقوانين واللوائح المصرية ذات الصلة.

وفيما يلي القوائم المالية المختصرة للشركة عن السنة المنتهية في 2022/12/31م:

1- قائمة المركز المالي المختصرة في 31 ديسمبر 2022:

(الأرقام بالمليون جنيه)

البيان	2021	2022
الأصول غير المتداولة	29000	28500
الأصول المتداولة	91500	89300
إجمالي الأصول	120500	117800
حقوق الملكية	32700	33600
الالتزامات غير المتداولة	12300	11600
الالتزامات المتداولة	74500	72600
إجمالي حقوق الملكية والالتزامات	120500	117800

2- قائمة الدخل المختصرة عن السنة المنتهية في 31 ديسمبر 2022:

(الأرقام بالمليون جنيه)

البيان	2021	2022
إيرادات النشاط	2000	1300
تكاليف النشاط	(1060)	(470)
مجمل الربح	940	830
إيرادات تشغيل أخري	140	90
مصروفات النشاط	(310)	(240)
الدخل التشغيلي	770	680
المصروفات التمويلية	(180)	(180)
صافي الأرباح قبل الضرائب	590	500
ضريبة الدخل	(132,75)	(112,5)
صافي أرباح العام	457,25	387,5

3- قائمة الدخل الشامل المختصرة عن السنة المنتهية في 31 ديسمبر 2022:

(الأرقام بالمليون جنيه)

البيان	2021	2022
أرباح العام	457,25	387,5
إجمالي الدخل الشامل الآخر بعد خصم الضريبة	19	-
إجمالي الدخل الشامل عن العام	476,25	387,5

4-قائمة التغير في حقوق الملكية المختصرة عن السنة المنتهية في 31 ديسمبر 2022:

(الأرقام بالمليون جنيه)

البيان	رأس المال المصدر والمدفوع	الاحتياطات	الأرباح المرحلة	إجمالي الدخل الشامل	توزيعات الأرباح	الإجمالي
الرصيد في 31 ديسمبر 2021	20600	1180,5	11620	387,5	(188)	33600
الرصيد في 31 ديسمبر 2022	20600	2663,75	10280	476,25	(320)	33700

5- قائمة التدفقات النقدية المختصرة عن السنة المنتهية في 31 ديسمبر 2022:

(الأرقام بالمليون جنيه)

البيان	2021	2022
صافي التدفقات النقدية من الأنشطة التشغيلية	800	(15)
صافي التدفقات النقدية من الأنشطة الاستثمارية	(400)	(355)
صافي التدفقات النقدية من الأنشطة التمويلية	700	(130)
صافي التغير في النقدية وما في حكمها	1100	(500)
رصيد النقدية وما في حكمها في بداية السنة	2700	3200
رصيد النقدية وما في حكمها في نهاية السنة	3800	2700

6- الإيضاحات المتممة للقوائم المالية

أسس إعداد القوائم المالية: يتم إعداد القوائم المالية وفقاً لمعايير المحاسبة المصرية وفي ضوء القوانين واللوائح المصرية السارية. وبالنسبة للتقديرات المحاسبية والافتراضات الرئيسية: يتم استخدام تقديرات معقولة كأساس لإعداد القوائم المالية وذلك وفقاً لمعايير المحاسبة المصرية, وتعتمد تقديرات الإدارة علي خبراتها التاريخية, ويتم مراجعتها بصورة دورية. وفيما يتعلق بالأصول الثابتة: يتم قياسها بالتكلفة التاريخية, ويتم احتساب الإهلاك بطريقة القسط الثابت. وبالنسبة للمعاملات التي تتم بالعملات الأجنبية: يتم تسجيلها بالدفاتر علي أساس سعر الصرف السائد للعملات الأجنبية وقت اثبات هذه المعاملات, وفي تاريخ الميزانية يتم إعادة تقييم أرصدة الأصول والالتزامات ذات الطبيعة النقدية بالعملات الأجنبية وفقاً لأسعار الصرف المعلنة في ذلك التاريخ, ويتم إدراج جميع الفروق الناتجة عن ذلك بقائمة الدخل الشامل. وبالنسبة لقائمة التدفقات النقدية: يتم إعدادها وفقاً للطريقة غير المباشرة.

في ضوء قراءتك للقوائم المالية السابقة وعلماً بأن تقرير مراجعة حسابات الشركة عن عام 2022 كان تقرير نظيف (غير متحفظ), وبصفتك مستثمر هل توافق علي ما يلي:

	العبارة / درجة الموافقة	موافق تماماً	موافق بدرجة كبيرة	موافق	غير موافق إلي حد ما	غير موافق تماماً
	سوف تستثمر في أسهم هذه الشركة.؟					
	إذا علمت أن سعر إقفال سهم الشركة في نهاية 2020, 2021, 2022 كان 0.53 , 1.27 , 0.90 علي التوالي فما هوتوقعك لسهر السهم في نهاية 2023: يثبت عند .....جنية. يزيد ليصبح .....جنية. يقل ليصبح .....جنية.					

الحالة التجريبية الثانية:

افترض نفس بيانات الحالة السابقة مع ملاحظة أن إدارة الشركة نشر التقرير التالي كإفصاح اختياري عن إدارة مخاطر الأمن السيبراني, وتم الإفصاح عنه ضمن مرفقات القوائم المالية لعام 2022, وظهر تقرير إدارة مخاطر الأمن السيبراني للشركة (س) كما يلي:

شركة "س" ش.م.م
تقرير إدارة مخاطر الأمن السيبراني عام 2022

السادة/ رئيس وأعضاء مجلس إدارة الشركة "س".
السادة/ مساهمي الشركة "س".

الفقرة التمهيدية:

قامت الشركة بالاستعانة بإطار إعداد تقرير إدارة مخاطر الأمن السيبراني الصادر عن المعهد الأمريكي للمحاسبين القانونيين (AICPA) في إعداد هذا التقرير. حيث إن برنامج إدارة مخاطر الأمن السيبراني للشركة يمثل مجموعة من السياسات والعمليات والضوابط المصممة لحماية المعلومات والأنظمة من الأحداث والهجمات الإلكترونية والوصول غير المصرح به, التي من الممكن أن تؤثر علي أداء عملها بشكل فعال وكفء.

تكوين برنامج إدارة مخاطر الأمن السيبراني من خلال الخطوات التالية:

- تم تحديد المخاطر الإلكترونية التي من الممكن أن تتعرض لها الشركة.
- تم تصميم وتفعيل هيكل رقابة للأمن السيبراني, لمعالجة المخاطر التي تم تحديدها في الخطوة الأولي ومتابعة خطط المعالجة.
- تم اختبار الفعالية التشغيلية لضوابط رقابة الأمن السيبراني, ومدي فاعليتها في صد الهجمات الإلكترونية.
- يتم عمل تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني واتخاذ الإجراءات التصحيحية. ويشرف مجلس الإدارة علي برنامج إدارة مخاطر الأمن السيبراني للشركة.

ولم تتعرض الشركة لأي هجمات إلكترونية في السنة المالية المنتهية في 2022/12/31, وذلك بفضل فعالية برنامج الأمن السيبراني لديها, والذي تمكنت الشركة من خلاله تحقيق أهداف الأمن السيبراني المتمثلة في الحفاظ علي سلامة وسرية توافر المعلومات.

التاريخ: 2023/4/21

عضو مجلس الإدارة المنتدب

في ضوء قراءتك للقوائم المالية, وتقرير إدارة مخاطر الأمن السيبراني, وبصفتك مستثمر هل توافق علي ما يلي:

	العبارة / درجة الموافقة	موافق تماماً	موافق بدرجة كبيرة	موافق	غير موافق إلي حد ما	غير موافق تماماً
	أن تقرير إدارة مخاطر الأمن السيبراني أثر علي قراراك الذي اتخذته في الحالة الأولي.					
	أن هذه الشركة ستكون لها الأولوية في الاستثمار في أسهمها مقارنة بالشركات المنافسة التي لم تنشر تقرير إدارة مخاطر الأمن السيبراني.					
	إذا علمت أن سعر إقفال سهم الشركة في نهاية 2020, 2021, 2022 كان 0.53 , 1.27 , 0.90 علي التوالي فما هوتوقعك لسهر السهم في نهاية 2023: يثبت عند .....جنية. يزيد ليصبح .....جنية. يقل ليصبح .....جنية.					