العدد الثالث– سبتمبر 2022– المجلد السادس

مجلة الإسكندرية للبحوث المحاسبية

قسم المحاسبة والمراجعة

أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية

أ.د/ محمود أحمد أحمد علي[1]

أستاذ المحاسبة والمراجعة

كلية التجارة– جامعة بني سويف

د/ صالح علي صالح علي[2]

مدرس المحاسبة والمراجعة

كلية التجارة – جامعة بني سويف

ملخص البحث

يهدف البحث إلى دراسة واختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية، وكذلك اختبار أثر بعض الخصائص الديمغرافية (مستوى الخبرة والتأهيل العلمي للمستثمر) كمتغيرات مُعدّلة على العلاقة محل الدراسة. ولتحقيق هدف البحث تم إجراء دراسة تجريبية على عينة من المستثمرين بالأسهم والمحللين الماليين في شركات السمسرة.

وخلصت الدراسة إلى وجود تأثير إيجابي ومعنوي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، كونه يضفي الثقة على أعمال الشركة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية. مما يُمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، مما يُسهم في ترشيد قرارات المستثمرين وتحسين جوده أحكامهم الاستثمارية.

كما خلص البحث إلى وجود تأثير معنوي لخبرة المستثمر ومستوى تأهيله العلمي على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم. كما أكدت نتائج التحليل الإضافي على أهمية الخصائص الديمغرافية للمستثمر في التأثير على أحكامه الاستثمارية. كما اتفقت نتائج تحليل الحساسية مع نتائج التحليل الأساسي عند حالة تغيير طريقة قياس المتغير التابع (قرار الاستثمار).

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

E.mail: drmahmoudgaafar@yahoo.com[1]

E.mail: saleh.aly679@gmail.com[2]

The Impact of disclosure of Cybersecurity Risk Management Report on the Investment Decision in Companies listed on the Egyptian Stock Exchange: Experimental Study

Abstract

The research aimed to study and test the impact of disclosure of Cybersecurity Risk Management Report on the investment decision in shares listed on the Egyptian Stock Exchange. The research also examined the impact of some demographic characteristics (investor qualification and experience level) on the relationship under study. To achieve the research objective, an experimental study was conducted on a sample of stock investors and financial analysts in brokerage firms.

The research concluded that there is a positive significant relationship between the Cybersecurity Risk Management Report and the stock investment decision, as it gives confidence to the company's work in the field of cybersecurity and protection from electronic attacks. This enables investors to assess the extent of the company's ability to maintain information security and reduce the possibility of breaches and negative events in the future, which contributes to rationalizing investors' decisions and improving the quality of their investment judgments.

The research also concluded that there is a significant effect of the investor's experience and the level of his scientific qualification on the relationship between the disclosure of the cybersecurity risk management report and the stock investment decision. Furthermore, the results of the additional analysis also confirmed the importance of the investor's demographic characteristics in influencing his investment judgments. Finally, the results of the sensitivity analysis were consistent with the results of the basic analysis when changing the method of measuring the dependent variable (investment decision).

Keywords: Cybersecurity - Cybersecurity Risk Management Report -Investment decision- Investor experience - Investor qualification.

1- مقدمة البحث

أدى الاعتماد المتزايد من جانب معظم الشركات حول العالم، على تقنيات وشبكات الويب في تخزين بياناتها الهامة على تلك الشبكات إلى زيادة احتمال تعرضها للهجمات السيبرانية (الإلكترونية) [1]، وهذا يجعل الأمن السيبراني مهمًا جدًا للشركات والمديرين وأعضاء مجلس الإدارة وأصحاب المصالح المتعددين والمتنوعين (Frank et al., 2019; Badawy, 2021). كما دعت بيئة الأعمال العالمية الشركات للحفاظ على بنية تحتية رقمية صالحة وآمنة لإجراء معاملاتها التجارية، تسمى البنية التحتية الرقمية المترابطة بالفضاء السيبراني وتشمل الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والمعلومات الرقمية. ويُعد هذا الفضاء الإلكتروني مهمًا للتجارة الإلكترونية والحكومة الإلكترونية والمعاملات الإلكترونية الأخرى (الاستراتيجية الوطنية للأمن السيبراني، 2017؛ Kahyaoglu & Caliyurt, 2018).

وتُعد تهديدات الأمن السيبراني، من أهم وأكثر التهديدات التي تواجه الشركات ومستقبلها، حيث أكد المديرين التنفيذيين (CEOs) لعدد من الشركات على التأثير السلبي لقضايا الأمن السيبراني على ثقة أصحاب المصلحة في الشركات وفي الصناعة (KPMG, 2018; PwC, 2019). حيث أن الهجوم الإلكتروني الذي يؤثر على تلف أو فقد بعض المعلومات المالية للشركات يكون له تأثير سلبي على ثروة الملاك وسمعة الشركة، نتيجة التأثير السلبي على أسعار أسهم الشركات وعلى تقييم أصحاب المصالح لمقدرة الشركة على الحفاظ على أمن المعلومات (Tuson, 2021; Kamiya et al., 2021). كما أنه من الممكن أن يمتد التأثير السلبي للهجمات الإلكترونية على فقد أصحاب المصالح الثقة في الشركة التي تعرضت للهجمات الإلكترونية وكذلك في الصناعة التي تنتمي إليها هذه الشركة، فيما يعرف بـ تأثير عدوى اختراق الأمن السيبراني (Cybersecurity Breach Contagion Effect) (Kelton & Pennington, 2020).

وبالتالي شهد موضوع الإفصاح عن الأمن السيبراني اهتماماً كبيراً من قبل العديد من الهيئات المهنية في الدول المختلفة، من خلال إصدار العديد من الإرشادات والتقارير المهنية في هذا الصدد، لدعم إفصاح الشركات عن مخاطر الأمن السيبراني وكيفية إدارة هذه المخاطر (SEC, 2011, 2018; AICPA, 2017; CSA, 2017; CPA-Canada, 2017). وفي البيئة العربية؛ أصدرت هيئة سوق المال السعودي في عام 2019 دليلاً إرشادياً للأمن السيبراني لمساعدة الشركات على إدارة مخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية في هذا الشأن. كما أصدر البنك المركزي الأردني في

[1] . حيث تم استخدام مصطلح (السيبراني/ السيبرانية/ الإلكتروني/الإلكترونية) في الاستراتيجية الوطنية المصرية للأمن السيبراني. وكذلك في الدليل الاسترشادي لهيئة سوق المال السعودي، وكذلك من البنك المركزي الأردني.

عام 2018 تعليمات للقطاع المالي والمصرفي من أجل التعامل مع مخاطر الأمن السيبراني. وفي 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؛ تعليمات التكيف مع المخاطر السيبرانية، 2018؛ الاستراتيجية الوطنية للأمن السيبراني، 2017).

وحظي أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وحوادث الأمن السيبراني على قرارات أصحاب المصالح وعلى أداء الشركات، باهتمام كبير من جانب الباحثين والجهات المهنية والأكاديمية. فقد أيدت بعض الدراسات (Frank et al., 2019; Cheng & Walton, 2019; Kelton & Pennington, 2020; Yang et al, 2020; Tuson, 2021; Kamiya et al, 2021; Perols & Murthy, 2021) وجود تأثير للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات بعض أصحاب المصالح مثل المحللين الماليين والمستثمرين، وكذلك على الأداء المالي للشركات وسمعتها. وإن كانت معظم هذه الدراسات تمت في أسواق رأس مال متقدمة ومتطورة، مما يستدعي دراسة أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات بعض أصحاب المصالح وخاصة المستثمرين في أسواق المال للدول النامية.

ومن ناحية أخرى، تناولت مجموعة من الدراسات السابقة (Bronwn et al., 2018; Espahodi et al., 2019; Pavlopouls et al., 2019; Akisik & Gal, 2020; Landau et al., 2020) تأثير الخصائص الديمغرافية للمستثمرين على قرار الاستثمار، حيث توصلت إلى وجود تأثير لتلك الخصائص، وخاصة خبرة ومستوى تأهيل المستثمر على قرار الاستثمار، ومن ثم كان من الأهمية دراسة أثر تلك الخصائص على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بالأسهم في مصر.

وفي مصر، يتضح عدم وجود تقنين للإفصاح عن إدارة مخاطر الأمن السيبراني أو قيام مراقب الحسابات بالتوكيد على هذا الإفصاح. حيث لا توجد أية معايير محاسبية أو معايير مراجعة مصرية تناولت ذلك الإفصاح بصورة مباشرة، وأنه ما زال الإفصاح عن إدارة مخاطر الأمن السيبراني في مصر اختيارياً (وإن حدث سيكون ضمن مرفقات القوائم المالية[2]). كما لا توجد أية متطلبات من سوق الأوراق

[1] . حيث يختلف مفهوم التقارير المالية عن مفهوم القوائم المالية، فقد عرف معيار المحاسبة المصري رقم (1) لعام 2015 القوائم المالية (Financial Statements) بأنها القوائم المعدة لمقابلة احتياجات المستخدم، الذي لا يكون في وضع يسمح له بطلب تقارير تعد خصيصاً للوفاء باحتياجاته. أما مفهوم التقارير المالية (Financial Reporting) فهو أوسع من مفهوم القوائم المالية إذ أنها تشمل بجانب

المالية المصرية للشركات المقيدة بالبورصة بتقديم مثل هذا النوع من الإفصاح. فهل إذا افصحت الشركات المقيدة بالبورصة المصرية عن تقرير إدارة مخاطر الأمن السيبراني سيؤثر ذلك الإفصاح على قرار الاستثمار بأسهم هذه الشركات، هذا ما سيجيب عنه البحث الحالي نظرياً وتجريبياً.

2- مشكلة البحث

نتيجة لتزايد الاهتمام بالإفصاح عن إدارة مخاطر الأمن السيبراني من جانب الباحثين في الأدب المحاسبي، وذلك لما له من تأثير واضح على أمن المعلومات ونجاح واستمرارية الشركات وتحسين جودة تقاريرها المالية (Cheng & Walton, 2019; Kelton & Pennington, 2020; Yang et al., 2020). الا أنه لم يحظ بالاهتمام الكافي من قبل التشريعات والقوانين والمعايير وقواعد القيد والشطب في البورصة المصرية، وأيضا الدراسات المصرية التي لم تتناول بشكل كاف، أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. **وعليه فيمكن التعبير عن مشكلة البحث في كيفية الإجابة نظريًا وتجريبياً على الأسئلة التالية:** ما المقصود بإدارة مخاطر الأمن السيبراني من منظور الإصدارات المهنية والدراسات السابقة؟ وكيف ولماذا يجب أن تقوم الشركات المقيدة بالبورصة بالإفصاح عن تقرير إدارة مخاطر الأمن السيبراني؟ وهل يؤثر المحتوى المعلوماتي لهذا الإفصاح على قرار الاستثمار بأسهم هذه الشركات؟ وهل يختلف هذا التأثير باختلاف خبرة المستثمر من جهة؟ ومستوى تأهيله العلمي من جهة أخرى؟ وهل يوجد دليل تجريبي على هذه العلاقات في بيئة الأعمال والممارسة المهنية في مصر؟ وإن وجد فما دلالاته المهنية؟

3- هدف البحث

يستهدف البحث دراسة واختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية، وكذلك اختبار أثر كل من مستوى الخبرة والتأهيل العلمي للمستثمر كمتغيرين معدلين للعلاقة محل الدراسة.

4- أهمية ودوافع البحث

تنبع أهمية البحث **الأكاديمية**، من أهمية الأمن السيبراني، ويسعى البحث إلى مواكبة توجهات المنظمات المهنية وجهات الإشراف والرقابة على أسواق المال العالمية والبحث المحاسبي في الدول المتقدمة في هذا المجال، وكذا التغلب على ندرة الدراسات المحاسبية، التي تناولت العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. كما تتمثل أهمية

القوائم المالية؛ الإفصاحات الأخرى خارج القوائم المالية، وتقرير مجلس الإدارة، وتقرير المسئولية الاجتماعية، والتقارير البيئية، وتقرير الاستدامة، وتقارير الحوكمة، وتقرير الإدارة عن الرقابة الداخلية.

البحث **العملية** في محاولة تقديم مقترح عن تقرير الشركة عن إدارة مخاطر الأمن السيبراني مشتق من الإصدارات والدراسات السابقة واختبار أثر الإفصاح عنه على قرار الاستثمار بالأسهم.

ومن أهم دوافع البحث التغلب على ندرة الدراسات المحاسبية المصرية، والحاجة إلى جهد الأكاديميين والممارسين في هذا المجال من جهة، ومحاولة تقديم إرشادات للجهات المهنية والتشريعية وهيئة الرقابة المالية والبورصة المصرية بشأن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني للمستثمرين، من جهة أخرى.

5- حدود البحث

يقتصر البحث على دراسة وتحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. ويركز البحث على دراسة بعض خصائص المستثمر (الخبرة ومستوى التأهيل) على العلاقة محل الدراسة. وبذلك يخرج عن نطاق البحث الخصائص الأخرى للمستثمر (مثل؛ النوع، العمر، الحالة الاجتماعية)، كما يخرج عن نطاق البحث اختبار العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرارات أصحاب المصالح الآخرين (مثل؛ مانحي الائتمان، جهات الإشراف والرقابة). وأخيرًا فإن قابلية نتائج البحث للتعميم مشروطة بضوابط منهجيته المستخدمة في اختبار فروضه، وخاصة ضوابط اختيار عينة البحث.

6- خطة البحث

لتحقيق هدف البحث، وفي ضوء مشكلته وحدوده، سوف يُستكمل البحث على النحو التالي:

6-1 تقرير إدارة مخاطر الأمن السيبراني (المفهوم والمكونات).

6-2 تحليل العلاقة بين المحتوي المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واشتقاق الفرض الرئيسي (وفرعياته).

6-3 منهجية البحث.

6-4 نتائج البحث والتوصيات ومجالات البحث المقترحة.

6-1 تقرير إدارة مخاطر الأمن السيبراني (المفهوم والمكونات)

تتمثل الأهداف العامة للأمن السيبراني (Cybersecurity) في الحفاظ على سرية المعلومات وسلامتها وتوافرها[3] (confidentiality, integrity, and availability). ويعرف الأمن السيبراني بأنه عبارة عن مجموعة من التقنيات والعمليات والممارسات التي تحمي وتضمن حماية أصول المنشأة (No & Vasarhelyi, 2017). ويعرف Craigen et al. (2014) الأمن السيبراني بأنه "تنظيم وجمع الموارد والعمليات والهياكل التي يتم استخدامها لحماية الفضاء الإلكتروني والأنظمة الأخرى التي تدعم الفضاء الإلكتروني من الهجمات والحوادث الإلكترونية".

وفي نفس السياق أكدت (الهيئة الوطنية للأمن السيبراني، 2018) على أن الأمن السيبراني هو مجموعة من التقنيات والعمليات التي تم تصميمها لحماية أجهزة الكمبيوتر والشبكات وقواعد البيانات والتطبيقات بما تحتويه من بيانات وما تقدمه من خدمات، من الهجمات الإلكترونية (Cyberattacks) والوصول غير المصرح به، والتغيير، أو تعطيل، أو سوء استخدام، أو استغلال غير مشروع. كما يؤكد (2020) Heroux & Anne على أن الأمن السيبراني يمثل مجموعة التقنيات والممارسات المصممة لحماية الشبكات والأنظمة وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التدمير أو الوصول غير المصرح به.

وفيما يتعلق بمخاطر الأمن السيبراني (cybersecurity risk)، تعتبر مخاطر الأمن السيبراني من أكبر المخاطر التي تواجهها الشركات، حيث على غرار المخاطر المالية ومخاطر السمعة التي تتعرض لها الشركات، يمكن لمخاطر الأمن السيبراني أن تؤدى الى ارتفاع التكاليف والتأثير السلبي على عوائد الشركات، والإضرار بقدرة الشركات على الابتكار واكتساب العملاء والحفاظ عليهم. حيث إن الهجمات الإلكترونية مكلفة ولها تأثير واضح على المركز المالي للشركات (Frank et al., 2019; Moshaigeh et al., 2019).

وعرفت (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 و/أو نظم المعلومات.

[1] . حيث تعرف **سرية المعلومة** بأنها "عملية الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والافصاح عنها، بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية". أما **سلامة المعلومة** يقصد بها " الحماية ضد أي تعديل أو تخريب للمعلومات بشكل غير مصرح به". في حين أن **توافر المعلومة** يقصد به "ضمان الوصل إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب" (الهيئة الوطنية للأمن السيبراني، 2018).

ونفس السياق قدمت دراسة Eaton et al.(2019) خمس خطوات يمكن من خلالها الحفاظ على برنامج فعال للإدارة مخاطر الأمن السيبراني، وتشمل هذه الخطوات؛ تحديد المخاطر الإلكترونية التي من الممكن أن تتعرض لها الشركة، وتصميم وتفعيل هيكل رقابة للأمن السيبراني، واختبار الفعالية التشغيلية لضوابط رقابة الأمن السيبراني، وإعداد تقرير عن إدارة مخاطر الأمن السيبراني، والحصول على توكيد مراقب الحسابات على تقرير إدارة مخاطر الأمن السيبراني.

كما قام البنك المركزي الأردني (Central Bank of Jordan) في عام 2018 بإصدار تعليمات للتعامل مع المخاطر السيبرانية. حيث تضمن الفصل الثالث تعليمات إدارة المخاطر السيبرانية؛ وشملت أولاً: تحديد العمليات الحرجة وأصول المعلومات الداعمة في الشركة، ثانياً: تقييم المخاطر السيبرانية، ويمكن للشركة الاستعانة بطرف ثالث لمساعدتها في عمليات تقييم المخاطر السيبرانية.

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

كما تم توصيف برنامج إدارة مخاطر الأمن السيبراني، من قبل المعهد الأمريكي للمحاسبين القانونيين American Institute of Certified Public Accountants (AICPA, 2018) بأنه مجموعة من السياسات والعمليات والضوابط المصممة لحماية المعلومات والأنظمة من الهجمات والاختراقات الإلكترونية التي يمكن أن تتعرض لها الشركة، وتُعرض تحقيق أهداف الأمن السيبراني للخطر، وتوضيح الاستجابة والتخفيف من تأثير الهجمات الإلكترونية التي لم يتم منعها في الوقت المناسب.

ويخلص الباحثان مما سبق إلى أن الأمن السيبراني، يشمل حماية الأنظمة والشبكات والبرامج وأصول المنشأة من الهجمات والحوادث الإلكترونية التي يمكن أن تؤثر على أداء عملها بشكل فعال وكفء، وذلك من أجل تحقيق أهداف الحفاظ على سرية المعلومات وسلامتها وتوافرها. **كما يقصد بإدارة مخاطر الأمن السيبراني،** قيام الشركات بتبني منهجية مناسبة تمكنها من تنفيذ وتشغيل ضوابط رقابية تساعدها على حماية أنظمتها وأصولها المعلوماتية. ولتحسين عملية إدارة هذه المخاطر، تحتاج الشركات إلى 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 على الشركة من الإدارة الفعالة لمخاطر الأمن السيبراني.

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

وفي الولايات المتحدة الأمريكية، قدم المعهد الأمريكي للمحاسبين القانونيين (2017) AICPA في أبريل 2017 إطارًا لإعداد تقرير إدارة مخاطر الأمن السيبراني (ضوابط النظام والمنظمة System and Organization Controls (SOC))، 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 إلى أصحاب المصالح. ولدعم الإطار تم إصدار مجموعتين من المعايير لوصف أهداف عمليات وضوابط الأمن السيبراني الفعالة التي يجب على الشركات تصميمها وتنفيذها للحصول على برنامج قوي وفعال لإدارة مخاطر الأمن السيبراني، وتشمل هذه المعايير:

1. معايير الوصف (Description Criteria): لاستخدامها من قبل إدارة الشركات لإعداد تقرير إدارة مخاطر الأمن السيبراني، مما يوفر معلومات تمكن مستخدمي التقرير من فهم مخاطر الأمن السيبراني للشركة وكيفية إدارتها لتلك المخاطر. وتشمل معايير الوصف العناصر التسعة التالية، والتي تتمثل في؛ (1) طبيعة أعمال الشركة وعملياتها، (2) الأنواع الرئيسية من المعلومات الهامة التي يتم تجميعها وإرسالها واستخدامها أو تخزينها بواسطة الشركة، (3) أهداف برنامج إدارة مخاطر الأمن السيبراني والتي تشمل الأهداف العامة للأمن السيبراني المتمثلة في الحفاظ على سرية المعلومات وسلامتها وتوافرها، (4) العوامل التي لها تأثير كبير على المخاطر الطبيعية (الحتمية) للأمن السيبراني، ومن أمثلتها خصائص التكنولوجيا التي تستخدمها الشركة، والتغيرات البيئية والتكنولوجية والتنظيمية التي حدثت خلال فترة وصف الشركة لبرنامج إدارة مخاطر الأمن السيبراني، (5) هيكل حوكمة إدارة مخاطر الأمن السيبراني وإشراف مجلس الإدارة على برنامج مخاطر الأمن السيبراني للشركة، (6) عملية إدارة مخاطر الأمن السيبراني، من خلال تحديد المخاطر الإلكترونية والتغيرات البيئية والتكنولوجية والتنظيمية التي يمكن أن يكون لها تأثيراً جوهرياً على برنامج إدارة مخاطر الأمن السيبراني للشركة وتقدير المخاطر المتعلقة بتحقيق الشركة لأهداف الأمن السيبراني، (7) قنوات اتصال الأمن السيبراني وجودة معلومات الأمن السيبراني، وتشمل عملية توصيل المعلومات للأطراف الداخلية المتعلقة بالأمن السيبراني واللازمة لدعم عمل برنامج إدارة مخاطر الأمن السيبراني للشركة، (8) ضوابط رقابة برنامج إدارة مخاطر الأمن السيبراني، وتشمل إجراء تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية

المتعلقة بالأمن السيبراني واتخاذ الإجراءات التصحيحية، (9) أنشطة مراقبة الأمن السيبراني، وتشمل عملية تطوير الاستجابة السريعة للمخاطر المتوقعة بما في ذلك تصميم وتنفيذ عمليات الرقابة.

2. معايير خدمات الثقة (Trust Services Criteria): منذ عام 1997 حافظ المعهد الأمريكي للمحاسبين القانونيين (AICPA) على مجموعة من المعايير التي تستخدم للتقييم والتقرير عن فعالية الضوابط المتعلقة بسلامة وسرية وتوافر المعلومات والأنظمة، وهذا يسمح للشركات استخدام معايير خدمات الثقة التي تم تنقيحها وتعديلها عام 2017 (معايير خدمات الثقة) كمعايير للرقابة، يمكن من خلالها التقييم والتقرير عن فعالية الضوابط المتعلقة بسلامة وسرية وتوافر المعلومات. هذا ويعد إطار التقرير مرن حيث يسمح للشركات باستخدام معايير أخرى غير معايير خدمات الثقة كمعايير للرقابة. مثل إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا في أمريكا (National Institute of Standards and Technology (NIST)). ومعايير (ISO 27001/27002) الصادرة عن المنظمة الدولية للمعايير.

ويتكون التقرير الذى سوف تُعده الشركات للإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني من ثلاثة أقسام (SOC, 2017):

القسم الأول: وصف الإدارة (Management's description): وهو عبارة عن وصف سردي تعده إدارة الشركة، لوصف برنامج إدارة مخاطر الأمن السيبراني بالاستعانة بمعايير الوصف التسعة (السابق عرضها).

القسم الثاني: تأكيد الإدارة (Management's assertion): ويشمل هذا القسم تأكيد تقدمه إدارة الشركة بأن إعداد ووصف التقرير يتم وفقاً لمعايير الوصف، كما تؤكد إدارة الشركة على فعالية ضوابط الرقابة على برنامج إدارة مخاطر الأمن السيبراني، وفقاً لمعايير خدمات الثقة (معايير الرقابة).

القسم الثالث: رأي (الممارس) مراقب الحسابات (The practitioner's opinion): ويحتوي هذا القسم على رأي مراقب الحسابات الذي قام بفحص ومراجعة تقرير إدارة مخاطر الأمن السيبراني الذي أعدته إدارة الشركة. ويستخدم مراقب الحسابات معايير الوصف والرقابة المحددة من قبل (AICPA) لكي يتمكن من تقييم ما إذا كانت الضوابط الرقابية داخل برنامج إدارة مخاطر الأمن السيبراني للشركة فعالة وتعمل كما يجب لتحقيق أهداف الأمن السيبراني المتمثلة في الحفاظ على سلامة وسرية وتوافر المعلومات. ومن ثم الحصول على أدلة إثبات كافية ومناسبة لتوفير أساس معقول لرأيه بشأن تقرير إدارة مخاطر الأمن السيبراني للشركة.

وفي عام 2018 أصدرت لجنة البورصة والأوراق المالية الأمريكية Securities and Exchange Commission (SEC) دليلاً يتضمن إرشادات للشركات المقيدة بالبورصة يتعلق بمتطلبات الإفصاح عن الأمن السيبراني. حيث يتكون من قسمين؛ **القسم الأول** يتناول مراجعة للقواعد التي تتعلق بالإفصاح عن مخاطر الأمن السيبراني ويتناول؛ الأهمية النسبية وعوامل الخطر والموقف المالي للشركة ونتائج العمليات ووصف طبيعة نشاط الشركة والإجراءات القانونية والإفصاح عن تعامل الشركة مع مخاطر الأمن السيبراني في القوائم المالية أو في مناقشات وتحليلات الإدارة (Management's Discussion and Analysis (MD&A)). ويتناول **القسم الثاني** السياسات والإجراءات التي تتبعها الشركات لرقابة وإدارة مخاطر الأمن السيبراني.

وفي كندا، قدم معهد المحاسبين القانونيين الكنديين (2017) CPA– Canada، وكذلك هيئة سوق الأوراق المالية الكندية (CSA, 2017) Canadian Securities Administrators إرشادات للشركات المقيدة بالبورصة تتعلق بكيفية الإفصاح عن مخاطر الأمن السيبراني، والإفصاح عن الآثار المحتملة لحوادث الأمن السيبراني، والإفصاح عن أنشطة الحوكمة للتحفيف من مخاطر وحوادث الأمن السيبراني. وذلك في القوائم المالية أو في مناقشات وتحليلات الإدارة من أجل توضيح الأمور ذات الأهمية النسبية والاتجاهات والمخاطر التي من المحتمل أن تؤثر على أداء الشركات في المستقبل، وكذلك مدى تأثير حوادث ومخاطر الأمن السيبراني على البيانات المالية للشركات.

وفي السعودية، أصدرت هيئة سوق المال السعودي في عام 2019 (هيئة سوق المالي السعودية، 2019) دليلاً إرشادياً للأمن السيبراني لمؤسسات السوق المالية، بهدف تحديد الضوابط المتعلقة بالأمن السيبراني للشركات السعودية المقيدة بالبورصة والتي تساعد على تحسين إدارة مخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية وتشريعات الأمن السيبراني السعودية. ثم تبعه بعد ذلك إصدار الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتكنولوجيا المعلومات في عام 2020.

وفي الأردن، أصدر البنك المركزي الأردني في عام 2018 (البنك المركزي الأردني، 2018) تعليمات التكيف مع مخاطر الأمن السيبراني كمفتاح رئيسي لرفع كفاءة القطاع المالي والمصرفي في الأردن في مواجهة التحديات والمخاطر السيبرانية.

وفيما يتعلق بالوضع في مصر، فقد نصت المادة (31) من الدستور المصري (يناير 2014) على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون". وبناءً على ذلك تم وضع الاستراتيجية الوطنية

للأمن السيبراني (2017–2021) من قبل المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء وبرئاسة وزير الاتصالات وتكنولوجيا المعلومات. ويتمثل الهدف الاستراتيجي لها في مواجهة المخاطر السيبرانية وتعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الالكترونية المتكاملة. وتشمل الاستراتيجية؛ **التحديات والأخطار السيبرانية** والتي تتمثل في خطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات، وخطر الإرهاب والحرب السيبرانية، وخطر سرقة الهوية الرقمية والبيانات الخاصة. **وأهم القطاعات الحيوية المستهدفة** وتشمل بالترتيب قطاع الاتصالات وتكنولوجيا المعلومات، قطاع الخدمات المالية، قطاع الطاقة، قطاع الخدمات الحكومية، قطاع النقل والمواصلات، وقطاع الاعلام والثقافة.

ويخلص الباحثان مما سبق إلى أن تقرير إدارة مخاطر الأمن السيبراني، يُعد أحد أشكال الإفصاح الاختياري الذي تستخدمه الشركات كوسيلة لتوصيل جهودها في مجال إدارة مخاطر الأمن السيبراني إلى أصحاب المصالح المتعددين والمتنوعين، والتأكيد على تحقيق الشركات لأهداف الأمن السيبراني المتمثلة في الحفاظ على سرية المعلومات وسلامتها وتوافرها. ويمكن للشركات استخدام إطار تقرير إدارة مخاطر الأمن السيبراني الذي قدمه (AICPA) للإفصاح عن هذا التقرير ضمن القوائم المالية للشركة أو في تقرير مجلس الإدارة (ضمن مرفقات القوائم المالية).

6-2 تحليل العلاقة بين المحتوي المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واشتقاق الفرض الرئيسي (وفرعياته)

سعت العديد من الدراسات السابقة (Hilary et al., 2016; Berkman et al., 2018; Frank et al., 2019; Heroux & Anne, 2020; Kelton & Pennington, 2020; Badawy, 2021; Perols & Murthy, 2021) إلى اختبار ما إذا كان الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني له مردود إيجابي على أصحاب المصالح وخاصة المستثمرين، وهذا ما سوف يتم تناوله على النحو التالي:

6-2-1 تحليل العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واشتقاق الفرض الرئيسي للبحث (H1)

أكدت بعض الدراسات (Hilary et al., 2016; Heroux & Anne, 2020; Kelton & Pennington, 2020) على أن الشركات يمكنها استخدام نظرية الإشارة Theory Signaling للحد من عدم تماثل المعلومات بين الإدارة وأصحاب المصالح، من خلال إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني لإرسال إشارات إيجابية لأصحاب المصالح حول الجهود المبذولة من الشركة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية. حيث إن الإفصاح عن تقرير إدارة مخاطر الأمن

السيبراني، يُمكن أصحاب المصالح من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل (Li et al 2018).

حيث سعت دراسة Berkman et al (2018) إلى اختبار العلاقة بين إفصاح الشركات عن برنامج إدارة مخاطر الأمن السيبراني وقيمة الشركة مقاسة بـ (Tobin's Q)، وذلك من خلال الاعتماد على أسلوب تحليل المحتوى لعينة من 9677 مشاهدة لعدد 2264 شركات مدرجة في بورصة الأوراق المالية الأمريكية خلال الفترة من 2012 إلى 2016. وخلصت الدراسة الى أن الإفصاح عن برنامج إدارة مخاطر الأمن السيبراني يؤثر بشكل إيجابي ومباشر على قيمة الشركة. وفي نفس السياق اتجهت دراسة Cheng & Walton (2019) إلى دراسة أثر الإفصاح عن تعرض الشركة للهجمات الإلكترونية على قرارات المستثمرين غير المحترفين، وذلك من خلال دراسة تجريبية تمت على عينة مكونة من عدد 107 مستثمر غير محترف من 32 ولاية في أمريكا. وتوصلت الدراسة إلى وجود علاقة سلبية بين تعرض الشركات للهجمات الإلكترونية وقرار الاستثمار في أسهمها.

وفي ذات السياق، استهدفت دراسة Tuson (2021) دراسة أثر الإفصاح عن تعرض الشركة للهجمات الإلكترونية على قيمة الشركة وسمعتها في الأجل القصير والأجل الطويل، وذلك من خلال الاعتماد على أسلوب تحليل المحتوى لعينة من 169 شركات مدرجة في بورصة الأوراق المالية الأمريكية خلال الفترة من 2004 إلى 2019. وخلصت الدراسة الى أنه عندما تفصح الشركات عن تعرضها لهجوم سيبراني لأول مرة فإنه توجد آثار على المدى القصير تتمثل في انخفاض العوائد اليومية وزيادة حجم التداول نتيجة ضغوط عمليات بيع أسهم الشركة. وكذلك توجد آثار على المدى الطويل حتى خمس سنوات تتمثل في تأثر سياسيات الشركة نتيجة الأضرار السلبية على قيمة الشركة وسمعتها. حيث إن الاختراقات الأمنية والهجمات السيبرانية ترتبط بعلاقة سلبية مع قيمة وسمعة الشركة، حيث يعكس ذلك مدى اهتمام الشركة بالحفاظ على أمن المعلومات.

وكذلك أكدت دراسة Kamiya et al. (2021) التي تمت على عينة مكونة من 244 شركة مدرجة في البورصة الصينية خلال الفترة من 2005 إلى 2017، على أن الهجوم الإلكتروني الذي يؤثر على تلف أو فقد بعض المعلومات المالية للشركات يكون له تأثير سلبي على ثروة الملاك وسمعة الشركة، نتيجة التأثير السلبي على أسعار أسهم الشركات وعلى تقييم أصحاب المصالح لمقدرة الشركة على الحفاظ على أمن المعلومات.

في حين اتجهت دراسة Spanos & Angelis (2016) إلى دراسة أثر الإفصاح عن معلومات الأمن السيبراني على أسعار الأسهم، وذلك من خلال القيام بدراسة نظرية تحليلية للعدد 45 دراسة. وخلصت

الدراسة إلى اتفاق 75.6% من هذه الدراسات على وجود علاقة إيجابية معنوية بين الإفصاح عن معلومات الأمن السيبراني وأسعار أسهم الشركات. وفي نفس السياق اتجهت دراسة Ali et al. (2021) إلى دراسة أثر الإفصاح عن تعرض الشركات للهجمات الإلكترونية وأحداث أمن المعلومات على أسعار أسهمها، وذلك من خلال القيام بدراسة نظرية تحليلية للعدد 80 دراسة. وخلصت الدراسة إلى اتفاق 75% من هذه الدراسات على وجود تأثير جوهري لإفصاح الشركات عن تعرضها للهجمات الإلكترونية وأحداث أمن المعلومات على أسعار أسهمها.

وفي نفس السياق، تناولت دراسة Yang et al. (2020) مدى إدراك المستثمرين لأهمية إطار إعداد تقرير إدارة مخاطر الأمن السيبراني الذي قدمه (AICPA) في عام 2017، وذلك من خلال دراسة تجريبية تمت على عينة مكونة من عدد 226 مستثمر غير محترف في الولايات المتحدة الأمريكية. وتوصلت الدراسة إلى أن إطار إعداد تقرير إدارة مخاطر الأمن السيبراني الذي قدمه المعهد الأمريكي للمحاسبين القانونيين، يُمكن الشركات من الإفصاح عن برنامج الأمن السيبراني لديها ويساعد على زيادة الوعي بالأمن السيبراني، وأن إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني طبقاً لهذا الإطار كان له تأثير إيجابي على تحسين قرارات المستثمرين، وساهم في زيادة ثقة المستثمرين في تلك الشركات. وفي ذات السياق، توصلت دراسة Kelton & Pennington (2020) إلى أن الإفصاح الاختياري عن برنامج إدارة مخاطر الأمن السيبراني له تأثير إيجابي على قرارات المستثمرين، وذلك من خلال دراسة تجريبية تمت على عينة مكونة من عدد 120 مستثمر غير محترف في الولايات المتحدة الأمريكية.

واستهدفت دراسة الرشيدي & السيد (2019) التعرف على طبيعة الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية للشركات المقيدة بالبورصة المصرية العاملة في قطاع تكنولوجيا المعلومات وأثرة على أسعار الأسهم وحجم التداول، ومقارنة ذلك مع الشركات الأمريكية التي تعرضت لهجمات إلكترونية مؤخراً. وتوصلت الدراسة إلى ضعف الإفصاح عن مخاطر الأمن السيبراني في الشركات المصرية مقارنة بالشركات الأمريكية، كما توصلت الدراسة لوجود تأثير سلبي للهجمات الإلكترونية على أسعار الأسهم وحجم التداول.

وفي اتجاه أخر، اتجهت بعض الدراسات (Frank et al., 2019; Badawy, 2021; Perols & Murthy, 2021) إلى دراسة أثر توكيد مراقب الحسابات على تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين. حيث توصلت دراسة Frank et al. (2019) إلى أن تأكيد الإدارة بشأن فعالية ضوابط الرقابة على برنامج إدارة مخاطر الأمن السيبراني، سيكون أكثر فعالية فقط في حالة عدم تعرض الشركة لهجوم إلكتروني حيث إن المستثمرين لن يشككوا في مصداقية الإدارة. أما في حالة تعرض الشركة لهجوم إلكتروني فإن توكيد مراقب الحسابات على تقرير إدارة مخاطر الأمن السيبراني سيكون أكثر فعالية

في تعزيز جاذبية الاستثمار وترشيد قرارات المستثمرين. وذلك من خلال دراسة تجريبية تمت على عدد 547 مستثمر غير محترف في الولايات المتحدة الأمريكية.

واستهدفت دراسة Badway (2021) دراسة أثر توكيد مراقب الحسابات على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين غير المحترفين، وذلك من خلال دراسة تجريبية تمت على عينة مكونة من عدد 64 طالب بمرحلة الدراسات العليا كممثلين للمستثمرين غير المحترفين في مصر. وتوصلت الدراسة إلى أن توكيد مراقب الحسابات كان له تأثير إيجابي ومعنوي على قرار الاستثمار. وفي نفس السياق، توصلت دراسة Perols & Murthy (2021) إلى وجود تأثير إيجابي لتوكيد مراقب الحسابات على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين، وذلك من خلال دراسة تجريبية تمت على عينة مكونة من عدد 106 طالب بمرحلة الدراسات العليا كممثلين للمستثمرين غير المحترفين في الولايات المتحدة الأمريكية.

ويخلص الباحثان مما سبق، أنه منهجيًا اختلفت هذه الدراسات في منهجيتها. حيث قد غلب على كثير منها إتباع المنهج التجريبي عند تناولها لمدى اهتمام المستثمرين بتقارير إدارة مخاطر الأمن السيبراني، وتأثيرها على قراراتهم، ومنها دراسات (Frank et al., 2019; Cheng & Walton, 2019; Kelton & Pennington, 2020; Yang et al., 2020; Badawy, 2021; Perols & Murthy, 2021). بينما اتبع البعض منهج تحليل المحتوى، مثل دراسات (الرشيدي & السيد، 2019; Berkman et al., 2018; Tuson, 2021; Kamiya et al., 2021). في حين اتبع البعض الأخر المنهج النظري التحليلي، مثل دراسات (Spanos & Angelis, 2016; Ali et al., 2021). وبالرغم من اختلاف منهجية البحث، إلا أن هذه الدراسات اتفقت على وجود أثر إيجابي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين.

ومن ناحية أخرى، ومن حيث البيئات التي أُجريت فيها هذه الدراسات، فقد أُجريت معظمها في بيئات دول مُتقدمة مثل الولايات المُتحدة الأمريكية، والصين. وقليل منها تم في بيئات الدول النامية مثل مصر مثل دراسات (الرشيدي & السيد، 2019; Badawy, 2021). ويبرر الباحثان ذلك بأن موضوع الأمن السيبراني حديث نسبياً، لذا فمن الطبيعي أن تهتم به الدول المتقدمة. ومن حيث عينة الدراسة، فقد اعتمدت بعض الدراسات على عينة من المستثمرين المحترفين، بينما اعتمد البعض الأخر على طلبة الدراسات العليا كممثلين للمستثمرين غير المحترفين. إلا أنها توصلت لنفس النتائج ووجدت تأثيرًا إيجابيًا على قرارات المستثمرين المتعلقة بتقييم الاستثمار، نتيجة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.

ويخلص الباحثان مما سبق، إلى اتفاق الدراسات السابقة على أن هناك اهتمامًا من جانب المستثمرين بتقرير إدارة مخاطر الأمن السيبراني، لأنه يساهم في الحد من ظاهرة عدم تماثل المعلومات بين الإدارة وأصحاب المصالح، عن طريق إرسال الشركات لإشارات إيجابية للمستثمرين وغيرهم من أصحاب المصالح حول الجهود المبذولة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية. مما يُمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل. مما يُساعد في تحسين كفاءة قرارات الاستثمار التي يتم اتخاذُها. بالإضافة إلى أنه يوفر الثقة في أعمال الشركة، وينعكس على الأداء المالي، وبالتالي يؤثر على سُمعة الشركة وأسعار الأسهم والتدفُق النقدي المُستقبلي. **ولذلك يتوقع الباحثان** أن يُساعد تقرير إدارة مخاطر الأمن السيبراني المستثمرين على ترشيد قراراتهم الاستثمارية، واتخاذ قرارات استثمارية مُستنيرة. **ولذا يمكن اشتقاق الفرض الرئيسي (H1) على النحو التالي:**

H1: يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني إيجابًا ومعنويًا على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

6-2-2 تحليل أثر اختلاف مستوى خبرة المستثمر على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واشتقاق الفرض الفرعي (H1a)

اتفقت بعض الدراسات (Bronwn et al., 2018; Espahodi et al., 2019;Pavlopouls et al., 2019; Akisik & Gal, 2020; Landau et al., 2020) على أن قرار الاستثمار يُعد دالة في العديد من العوامل المرتبطة بالشركة، أو بالصناعة، أو بالدولة، أو بالمستثمر نفسه. حيث يتأثر قرار الاستثمار بخصائص المستثمر نفسه مثل خبرته ومستوى تأهيله العلمي، وهو ما يؤثر على حكمه الشخصي، ومن ثم على قراره. ويؤثر اختلاف مستوى الخبرة بين المستثمرين على إدراكهم وفهمهم للمحتوي المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني، مما يؤدي إلى التباين في قرارهم بشأن الاستثمار في أسهم نفس الشركة، نتيجة اختلاف تقييمهم لأسهم الشركات، حيث يختلف رد فعل المستثمرين ذوي الخبرة عن قليلي الخبرة تجاه تقرير إدارة مخاطر الأمن السيبراني، ويكون رد فعل المستثمرين ذوي الخبرة أكثر سرعة وأكبر تأثيرًا.

وفي نفس السياق، توصلت دراسة Christanti & Mahastanti (2011) من خلال الدليل التجريبي، إلى أن مستوى التعليم والخبرة بالاستثمار تؤثر على قرار الاستثمار في الأسهم. كما أشارت دراسة Lan et al (2018) من خلال دراسة تمت على عدد 9000 مستثمر فرد في الصين، إلى وجود تأثير معنوي للخصائص الديمغرافية للمستثمر (خبرة المستثمر ومستوى تأهيله العلمي) على سلوكه الاستثماري. كما أوضحت دراسة Reimsbach et al. (2018) أن أحكام المستثمرين تعتمد على خبرتهم وبعض عواملهم

النفسية. كما توصلت دراسة كل من (موسى، 2018، علي، 2019) إلى أنه كلما زاد مستوى خبرة المستثمر كلما زاد إدراكه لمحتوى التقارير غير المالية التي تصدرها الشركات، ووجدوا تأثير إيجابي لخبرة المستثمر على العلاقة بين الإفصاح عن المعلومات غير المالية وقرار الاستثمار في الأسهم.

ويخلص الباحثان مما سبق، أن هناك اتفاقًا بين الدراسات السابقة على أن هناك تأثيرًا واضحًا لخبرة المستثمر على قراراته، حيث تختلف قرارات المستثمرين باختلاف خبرتهم في مجال الاستثمار بالأسهم. كما أن هناك نُدرة في الدراسات التي تناولت أثر خبرة المستثمر على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار، مما يبرر أهمية البحث في هذا المجال. ويعتقد الباحثان أن خبرة المستثمر تساهم في تحسين إدراكه للمحتوي المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني، وتقييمه للمخاطر المختلفة التي تواجه الشركة، مما يساهم في تحسين جودة أحكامه الاستثمارية. **ولذلك يتوقع الباحثان** أن تؤثر خبرة المستثمر على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار. وعليه يمكن اشتقاق الفرض الفرعي (H1a) كما يلي:

H1a: يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى خبرة المستثمر.

6-2-3 تحليل أثر اختلاف مستوى التأهيل العلمي للمستثمر على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واشتقاق الفرض الفرعي (H1b)

تؤكد بعض الدراسات (Miazee & Hasan, 2014; Rena et al., 2016; Hoang & Phang, 2021) على أهمية التأهيل العلمي لمتخذ القرار بصفة عامة، والمستثمرين بصفة خاصة، في تكوين المعرفة والمهارة، التي يمكن أن تساهم في تحسين فهمهم وتقييمهم للمعلومات التي تفصح عنها الشركات، مما يؤدى إلى تحسين جودة قراراتهم. حيث إنه كلما ارتفع مستوى التعليم كلما زادت درجة تحمل المستثمر للمخاطر في قراراته الاستثمارية، حيث إن المستثمرين المؤهلين علمياً لديهم المزيد من المعرفة والمهارات المفيدة في قرار الاستثمار والتي تؤدي إلى تحسين جودة أحكامهم الاستثمارية مقارنة بالمستثمرين غير المؤهلين. كما أكدت دراسة Mishra & Metilda (2015) على أن من أهم الخصائص الديموغرافية لأصحاب المصالح، والتي تؤثر على قراراتهم هي: النوع، العمر، مستوى التأهيل العلمي، ومستوى الخبرة. ويؤثر التأهيل العلمي لأصحاب المصالح بدرجة كبيرة على سلوكهم، فهناك علاقة إيجابية معنوية بين الشهادات العلمية التي حصل عليها أصحاب المصالح وجودة قراراتهم.

حيث يعتبر التعليم أحد العوامل المؤثرة على قرارات الاستثمار، فكلما ارتفع مستوى التعليم فإن قرار الاستثمار سيعطي الفائدة المثلي والعائد المتوقع، حيث إن المستثمر الذي يتمتع بمستوى عال من التعليم لديه المزيد من المعرفة والمهارات المفيدة في قرار الاستثمار، حيث يكون العائد على الاستثمار مؤشراً لتحسن أداء الاستثمار للمستثمرين (Lutfi, 2010; Obamuyi, 2013). وفي نفس السياق توصلت دراسة كل من (موسى، 2018، علي، 2019) إلى وجود تأثير إيجابي لمستوى التأهيل العلمي المستثمر على العلاقة بين الإفصاح عن المعلومات غير المالية وقرار الاستثمار في الأسهم.

ويخلص الباحثان مما سبق، إلى أن مستوى التأهيل العلمي للمستثمر ذو تأثير معنوي على العلاقة محل الدراسة، فكلما زاد مستوى التأهيل العلمي للمستثمر كلما تحسن إدراكه وفهمه لمحتوى تقرير إدارة مخاطر الأمن السيبراني، مما يؤثر إيجابًا على تحسين جودة قراره الاستثماري. **ولذلك يتوقع الباحثان** أن يؤثر مستوى التأهيل العلمي للمستثمر على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم. وعليه يمكن اشتقاق الفرض الفرعي (H1b) كما يلي:

H1b: يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى التأهيل العلمي للمستثمر.

ونظراً لأهمية المتغيرين السابقين كمتغيرين معدلين للعلاقة محل الدراسة، ومن ثم يوجد سؤال منطقي، هل يختلف أثر هذين المتغيرين المعدلين مجتمعين (التفاعل بين خبرة المستثمر ومستوى تأهيله العلمي) على العلاقة محل الدراسة، مقارنة بأثر كل متغير منهم على حده. وبالتالي يرى الباحثان أنه من المنطقي أن نتوقع تأثيراً أكبر لمتغيري خبرة المستثمر ومستوى تأهيله العلمي معاً على العلاقة محل الدراسة مقارنة بتأثير كل منهما على حده. ومن ثم يمكن اشتقاق الفرض الفرعي (H1c) كما يلي:

H1c: يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى الخبرة والتأهيل العلمي للمستثمر معاً.

3-6 نموذج منهجية البحث

يعرض الباحثان في هذا القسم أهداف الدراسة التجريبية، ومجتمع وعينة الدراسة، نموذج الدراسة ومتغيرات الدراسة وكيفية قياسها بالإضافة إلى التصميم التجريبي وأخيراً الاختبارات الإحصائية اللازمة لاختبرا فروض الدراسة، وذلك على النحو التالي:

6-3-1 أهداف الدراسة التجريبية

تستهدف الدراسة التجريبية اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية، وكذلك اختبار أثر مستوى التأهيل العلمي وخبرة المستثمر كمتغيرين معدلين للعلاقة الرئيسية محل الدراسة.

6-3-2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من المستثمرين المحترفين، ويمثلهم أمناء الاستثمار ببعض البنوك التجارية ومعاونيهم، ومديرو الاستثمار بصناديق الاستثمار بالأسهم، والمحللين الماليين في شركات السمسرة وتداول الأوراق المالية. حيث تم سحب عينة منهم تضم 100 مفردة من المستثمرين. قياساً على (علي، 2019؛ Reimsbach et al, 2018; Hoang & Phang, 2021). ويوضح الجدول التالي عدد الحالات التجريبية الموزعة على عينة الدراسة بالإضافة إلى عدد ونسبة الردود، وكذلك عدد ونسبة الردود السليمة التي خضعت للتحليل الاحصائي.

جدول 1: بيان بالردود على الحالات التجريبية

بيان	عدد الحالات التجريبية الموزعة	عدد الحالات التجريبية المستلمة	نسبة الردود على الحالات المستلمة إلى الحالات الموزعة	عدد الردود الصادقة[4]	نسبة الردود الصادقة إلى الردود المستلمة
عينة المستثمرين في الأسهم	100	69	%69	63	%91.3

6-3-3 أدوات وإجراءات الدراسة

تتضمن أدوات الدراسة كل من؛ المقابلات الشخصية، والحالات التجريبية المبنية على التقارير المالية الفعلية لأحدى الشركات المقيدة بالبورصة المصرية، وتقرير إدارة مخاطر الأمن السيبراني، والأسئلة المرافقة لهذه الحالات، والاجابة على هذه الأسئلة (الملحق رقم 1) قياساً على (علي، 2019، محمد، 2020).

واعتمد الباحثان على التصميم التجريبي (2×2×2) قياساً على (Badawy, 2021; Perols & Murthy, 2021) بهدف اختبار العلاقة محل الدراسة، حيث تم صياغة نموذج قياسي مقترح للتقرير عن إدارة مخاطر الأمن السيبراني، وتم تحديد المتغيرين المعدلين الذي يفترض أن يؤثرا على العلاقة محل الدراسة وهما خبرة المستثمر ومستوى تأهيله العلمي. وبعد تصميم الحالات التجريبية أصبحت تتضمن الأقسام التالية: (الملحق رقم 1)

[1] . حيث تضمنت الحالة التجريبية سؤالاً يختبر صدق الردود واختبار العلاقة محل الدراسة معاً. حيث تم سؤال الأفراد عن أثر المتغير المستقل على سعر السهم المتوقع، فإن أجاب يثبت لا يجوز أن يختار يزيد أو يقل.

القسم الأول: البيانات الديمغرافية، وتشمل الخبرة وتأهيل المستثمر.

القسم الثاني: الحالة التجريبية الأولى: وتشمل قوائم مالية فعلية لشركة مساهمة مقيدة بالبورصة وتعمل في مجال الاستثمارات المالية عن سنتي (2019، 2020)، وتم تحويل القوائم المالية إلى قوائم مالية مختصرة، كما تم اختصار الإيضاحات المتممة بما لا يخل من الهدف منها.

القسم الثالث: الحالة التجريبية الثانية: وتشمل قوائم مالية فعلية لشركة مساهمة مقيدة بالبورصة وتعمل في مجال الاستثمارات المالية عن سنتي (2019، 2020)، ومرفق معها نموذج لتقرير مقترح لإفصاح الشركة عن برنامج إدارة مخاطر الأمن السيبراني.

ويرافق الحالات التجريبية مجموعة من الأسئلة للحصول على استجابات المشاركين في التجربة لمتغيرات الدراسة، من خلال مطالبتهم بالإجابة عن بعض التساؤلات التي تعكس استعدادهم للاستثمار في أسهم الشركة، وكذلك التنبؤ بسعر سهم الشركة في نهاية الفترة التالية.

6-3-4 توصيف وقياس متغيرات الدراسة

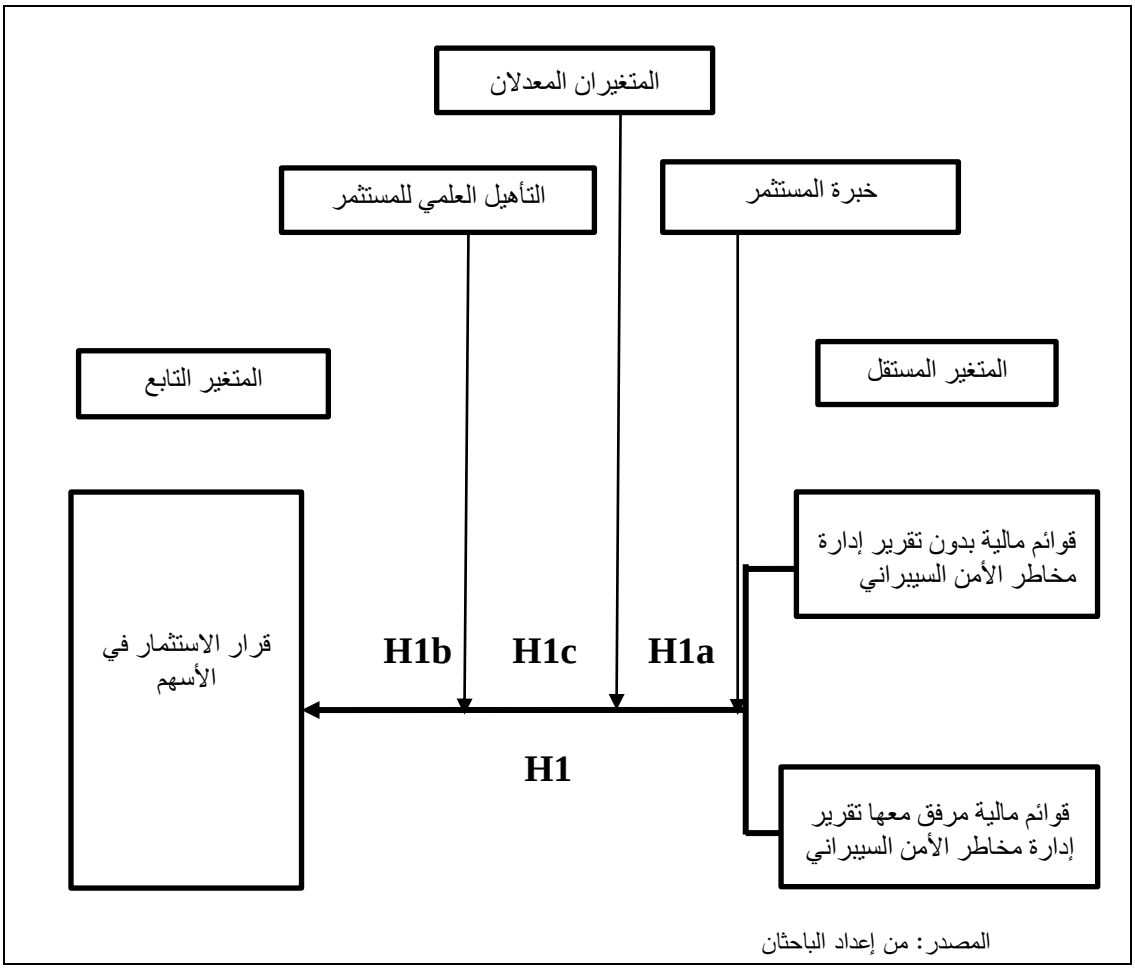
يوضح الجدول التالي توصيف وكيفية قياس متغيرات الدراسة كالتالي:

جدول 2: قياس وتوصيف متغيرات الدراسة

المتغير	نوعه	التوصيف	القياس
الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.	مستقل	تقرير يهدف إلى توصيل معلومات عن مزاعم وتأكيدات الإدارة بشأن تقييمها لفعالية ضوابط الرقابة المصممة على برنامج إدارة مخاطر الأمن السيبراني. من خلال تقرير ضمن مرفقات القوائم المالية (Yang et al., 2020).	من خلال إمداد أفراد العينة بتقرير عن إدارة مخاطر الأمن السيبراني مرفق بالقوائم المالية، ومقارنته بالوضع بدون تقرير إدارة مخاطر الأمن السيبراني (موسى، 2018، علي،2019، رميلي، 2020).
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 على الاستثمار (شحاته، 2014).	بتوقع سعر السهم للشركة في نهاية الفترة التالية واتخاذ قرار الاستثمار بالسهم (موسى، 2018، علي،2019).
مستوى خبرة المستثمر	معدل	يقصد بها درجة الدراية والمعرفة والخبرة لدى المستثمر، وقدرته على التحليل الدقيق والشامل للمعلومات الهامة ذات الصلة، واتخاذ قرار الاستثمار على أساسها (Reimsbach et al., 2018).	يقاس بعدد سنوات الممارسة الفعلية التي قضاها المستثمر في ممارسة عمله، وتأخذ القيمة (صفر) إذا كانت أقل من عشر سنوات، وتأخذ القيمة (1) إذا كانت تساوى أو أكبر من عشر سنوات (موسى، 2018، محمد، 2020).
مستوى التأهيل العلمي للمستثمر	معدل	يقصد به المؤهلات العلمية والشهادات المهنية التي حصل عليها المستثمر، والتي تؤهله لاتخاذ قرار الاستثمار بكفاءة وفعالية (علي، 2019، رميلي 2020).	ويعتبر المستثمر ذو تأهيل علمي مرتفع إذا حصل على دراسات عليا أو شهادات مهنية ويأخذ القيمة (1)، وذو تأهيل علمي منخفض بخلاف ذلك ويأخذ القيمة (صفر) (علي، 2019، محمد، 2020).

6-3-5 نموذج البحث

ويظهر نموذج البحث في الشكل التالي:



المصدر: من إعداد الباحثان

6-3-6 التصميم التجريبي والمعالجات والمقارنات

لاختبار فرض البحث الرئيسي وفرعياته تم استخدام التصميم التجريبي (2×2×2) التالي:

جدول 3: التصميم التجريبي للدراسة

سمات المستثمر / بدائل الإفصاح	مستوى خبرة المستثمر		مستوى التأهيل العلمي للمستثمر	
	ذو خبرة	قليل الخبرة	مؤهل	غير مؤهل
قوائم مالية فقط	المعالجة (1) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (2) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (3) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (4) قرار الاستثمار والتنبؤ بسعر السهم
قوائم مالية مرفق بها تقرير إدارة مخاطر الأمن السيبراني	المعالجة (5) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (6) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (7) قرار الاستثمار والتنبؤ بسعر السهم	المعالجة (8) قرار الاستثمار والتنبؤ بسعر السهم

وبناءً على هذا التصميم، هناك ثماني معالجات تجريبية كما يلي:

المعالجة (1): قوائم مالية فقط بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر ذو خبرة/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (2): قوائم مالية فقط بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر قليل الخبرة/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (3): قوائم مالية فقط بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر مؤهل/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (4): قوائم مالية فقط بدون تقرير إدارة مخاطر الأمن السيبراني/ مستثمر غير مؤهل/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (5): قوائم مالية + تقرير إدارة مخاطر الأمن السيبراني/ مستثمر ذو خبرة/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (6): قوائم مالية + تقرير إدارة مخاطر الأمن السيبراني/ مستثمر قليل خبرة/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (7): قوائم مالية + تقرير إدارة مخاطر الأمن السيبراني/ مستثمر مؤهل/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

المعالجة (8): قوائم مالية + تقرير إدارة مخاطر الأمن السيبراني/ مستثمر غير مؤهل/ قرار استثمار في أسهم الشركة والتنبؤ بسعر السهم.

ولاختبار الفرض الرئيسي للبحث وفروضه الفرعية تم إجراء المقارنات الأربعة التالية:

المقارنة الأولى: بين المعالجات (1+2+3+4) والمعالجات (5+6+7+8) وذلك لقياس الأثر الإيجابي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، ومن ثم اختبار الفرض الرئيسي للبحث **(H1)**.

المقارنة الثانية: بين **[**(1×5)**]** × **[**(2×6)**]** وذلك لقياس أثر اختلاف التأثير الإيجابي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف مستوى خبرة المستثمر، ومن ثم اختبار الفرض الفرعي **(H1a)**.

المقارنة الثالثة: بين **[**(3×7)**]** × **[**(4×8)**]** وذلك لقياس أثر اختلاف التأثير الإيجابي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف مستوى التأهيل العلمي للمستثمر، ومن ثم اختبار الفرض الفرعي **(H1b)**.

المقارنة الرابعة: بين **[**(1+3) × (5+7)**]** × **[**(2+4) × (6+8)**]** وذلك لقياس أثر اختلاف التأثير الإيجابي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف الأثر المجمع لكل من خبرة المستثمر ومستوى تأهيله العلمي معاً، ومن ثم اختبار الفرض الفرعي **(H1c)**.

6-3-7 نتائج الدراسة التجريبية

6-3-7-1 الأساليب الاحصائية المستخدمة لتحليل نتائج الدراسة التجريبية

استخدم الباحثان العديد من الاختبارات الإحصائية التي تتناسب مع طبيعة بيانات الدراسة التجريبية وفروض البحث، وذلك كما يلي:

6-3-7-1-1 اختبار الصدق والثبات (Cronbach's Alpha)

تم اجراء اختبار كرونباخ ألفا Cronbach's Alpha لقياس الصدق والثبات، حيث يقيس هذا الاختبار مدى ثبات اجابات افراد العينة على الاسئلة المقدمة لهم، واختبار مدى الموثوقية في استجاباتهم، ومدى صلاحية بيانات الدراسة للتحليل الاحصائي لمعرفة مدى امكانية تعميم النتائج التي تم الحصول عليها من العينة على مجتمع الدراسة. ويأخذ هذا المعامل قيماً تتراوح بين الصفر والواحد الصحيح (0-1) وإذا كانت البيانات بها ثبات فإن هذا المعامل يكون مساوياً للواحد الصحيح، واذا كان هذا المعامل مساوياً للصفر

فهذا يعنى عدم ثبات البيانات. ويشير الثبات الى استقرار المقياس وعدم تناقضه مع نفسه، أي أن المقياس يعطى نفس النتائج باحتمال مساو لقيمة المعامل إذا أعيد تطبيقه على نفس العينة (عزام وزغلول، 2006). وتعتبر الزيادة في قيمة معامل الاختبار السابق معبرة عن الصدق بمعني صحة العلاقة السببية بين المتغير المستقل والتابع (الصدق الداخلي Internal Validity) ومن ثم إمكانية تعميم النتائج (الصدق الداخلي External Validity) وتقبل قيمة المعامل اذا تجاوزت 50% وهو ما تحقق في هذا البحث، حيث أظهرت النتائج أن قيمة معامل كرونباخ ألفا (.796) وهو ما يمثل مستوى جيداً من الصدق والثبات.

جدول 4: معامل كرونباخ ألفا لعينة الدراسة

Reliability Statistics

Sample	Cronbach's Alpha	N of Items
المستثمرون	0.796	5

6-3-7-1-2 تحديد نوع توزيع المجتمع Test of Normality

لتحديد نوع توزيع المجتمع، الذى تم سحب عينة الدراسة منه، وذلك من أجل تحديد ما اذا كان سيتم استخدام الاختبارات المعلمية Parametric Tests أو الاختبارات اللامعلمية Non Parametric Tests، تم اجراء اختبار Kolmogorov–Smirnov لمعرفة ما اذا كان هذا التوزيع يتبع التوزيع الطبيعي أم لا(عزام وزغلول،2006). وأظهرت نتائج هذا الاختبار أن قيمة P.Value أقل من 5% (.000) لجميع المتغيرات محل الدراسة. مما يعنى رفض الفرض العدم (القائل بأن المجتمع الذى سحبت منه عينة الدراسة يتبع التوزيع الطبيعي) وقبول الفرض البديل (القائل بأن المجتمع الذى سحبت منه عينة الدراسة لا يتبع التوزيع الطبيعي). **وبناءً على ذلك تم الاعتماد على الاختبارات اللامعلمية لاختبار فروض البحث.** ويوضح الجدول التالي نتائج هذا الاختبار.

جدول 5: نتائج اختبار توزيع بيانات عينة الدراسة

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
A1	.526	63	.000	.333	63	.000
A2	.409	63	.000	.610	63	.000
B1	.295	63	.000	.791	63	.000
B2	.364	63	.000	.715	63	.000
B3	.480	63	.000	.513	63	.000
a. Lilliefors Significance Correction						

6-3-7-2 نتائج اختبار فروض الدراسة

فيما يلي يعرض الباحثان لنتائج اختبار الفرض الرئيسي للبحث وفرعياته، وذلك على النحو التالي:

6-3-7-2-1 نتيجة اختبار الفرض الرئيسي للبحث (H1)

استهدف الفرض الرئيسي (H1) اختبار ما إذا كان الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يؤثر إيجاباً ومعنويًا على قرار الاستثمار في الأسهم، واستخدم الباحثان في هذا الشأن اختبار ويلكوكسون Wilcoxon Signed-Rank Test اللامعلمى لعينتين مرتبطتين (غير مستقلتين) لإجراء المقارنات الثنائية وتحديد مدى الاختلاف بين وسيطي العينتين. ولاختبار هذا الفرض تم تحويله الى صورة فرض العدم كما يلي:

H_0: لا يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني إيجابًا ومعنويًا على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

ويظهر الفرض الإحصائي الخاص بهذا الاختبار كما يلي:

فرض العدم: $M_1=M_2$:H_0: أي لا يوجد اختلافات معنوية في ردود عينة المستثمرين على الحالات التجريبية.

الفرض البديل: $M_1 \neq M_2$:H_1: أي يوجد اختلافات معنوية في ردود عينة المستثمرين على الحالات التجريبية.

ووفقًا لهذا الاختبار إذا كانت قيمة P.Value أقل من 5%، فيعني ذلك رفض فرض العدم وقبول الفرض البديل، أما إذا كانت قيمة P.Value أكبر من 5%، فيعني ذلك قبول فرض العدم ورفض الفرض البديل. وذلك وفقاً لنتائج الاختبار الموضحة في الجدول رقم (6) على المقارنة الأولى.

جدول 6: نتائج اختبار الفرض الرئيسي للبحث (H1)

Test Statistics[a]	
	B_ - A
Z	-6.069[b]
Asymp. Sig. (2 tailed)	.000
a. Wilcoxon Signed Ranks Test	
b. Based on negative ranks.	

ويتضح من الجدول رقم (6) أن قيمة (P.Value) هي (.000) أقل من مستوى المعنوية (5%)، مما يعني رفض الفرض العدم وقبول الفرض البديل. ومن ثم يمكن القول بوجود تأثير إيجابي ومعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين بالاستثمار في أسهم الشركات المقيدة

بالبورصة المصرية. وتتفق هذه النتيجة مع بعض الدراسات السابقة (Frank et al., 2019; Cheng & Walton, 2019; Kelton & Pennington, 2020; Yang et al., 2020; Badawy, 2021; Perols & Murthy, 2021). حيث إن تقرير إدارة مخاطر الأمن السيبراني لـه محتوى معلوماتي كونه يحد من ظاهرة عدم تماثل المعلومات، ويزيد من ثقة ودرجة اعتماد المستثمرين على هذه المعلومات عند اتخاذ قرار الاستثمار. بالإضافة إلى أنه يُمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل. مما يُساعد في تحسين كفاءة قرارات الاستثمار التي يتم اتخاذُها. بالإضافة إلى أنه يوفر الثقة في أعمال الشركة، وينعكس على الأداء المالي، وبالتالي يؤثر على سُمعة الشركة وأسعار الأسهم والتدفق النقدي المُستقبلي.

كما يتضح من الجدول التالي رقم (7) أن الرتب (Ranks) كانت لصالح الحالية الثانية وهي إرفاق تقرير إدارة مخاطر الأمن السيبراني، بما يعني أن اتجاه استجابات المستثمرين هي ضرورة توفير تقرير إدارة مخاطر الأمن السيبراني ضمن مرفقات القوائم المالية للشركات، للمساعدة على اتخاذ قرار الاستثمار في الأسهم. حيث يتضح أن هناك اهتماماً من جانب المستثمرين بالمعلومات التي يوفرها تقرير إدارة مخاطر الأمن السيبراني لأهميتها في تقييم الفرص الاستثمارية في ظل الثورة الصناعية الرابعة.

جدول 7: Wilcoxon Signed Ranks Test

Ranks				
		N	**Mean Rank**	**Sum of Ranks**
B- A	Negative Ranks	4[a]	8.25	33.00
	Positive Ranks	48[b]	28.02	1345.00
	Ties	11[c]		
	Total	63		
a. B< A				
b. B> A				
c. B = A				

6-3-7-2-2 نتيجة اختبار الفرض الفرعي (H1a)

استهدف الفرض الفرعي (H1a) اختبار ما إذا كان مستوى خبرة المستثمر كمتغير معدل يؤثر معنويًا على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واستخدم الباحثان في هذا الشأن اختبار ويلكوكسون Wilcoxon Signed-Rank Test اللامعلمى لعينتين مرتبطتين (غير مستقلتين) لإجراء المقارنات الثنائية وتحديد مدى الاختلاف بين وسيطي العينتين. ولاختبار هذا الفرض تم تحويله الى صورة فرض العدم كما يلي:

H_0: لا يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى خبرة المستثمر.

ويتضح نتائج هذا الاختبار في الجدول رقم (8) على المقارنة الثانية.

جدول 8: نتائج اختبار الفرض الفرعي (H1a)

الفرض		الاختبار الاحصائي	الاختبار المستخدم	N	Z	P-value
H1a	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى خبرة المستثمر.	أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين ذوي الخبرة.	Wilcoxon Signed Ranks Test	36	4.612	0.000
		أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين قليلي الخبرة.		27	3.836	0.000

تشير نتائج الاختبار (جدول رقم 8) إلى أن كل من المستثمرين ذوي الخبرة وقليلي الخبرة يستجيبون بصورة معنوية للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني عند تقييم أسعار الأسهم واتخاذهم لقرار الاستثمار في الأسهم، حيث كانت قيمة (P–value) (.000) أقل من (5%). وهذا يعني أن مستوى خبرة المستثمر كان لها تأثير معنوي على العلاقة بين المحتوى المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

وقام الباحثان بإجراء مقارنة بين الحالات السابقة باستخدام قيمة(Z) المحسوبة، لتحديد مدى قوة تأثير مستوى الخبرة على العلاقة محل الدراسة، من خلال مقارنة قيمة(Z) المحسوبة في الحالة الأولي بالحالة الثانية، فكلما زادت قيمة(Z) المحسوبة، دل ذلك على قوة تأثير مستوى خبرة المستثمر على العلاقة محل الدراسة. وبالرجوع إلى النتائج نلاحظ أن قيمة (Z) المحسوبة في حالة المستثمرين ذوي الخبرة **أكبر من** قيمة (Z) المحسوبة في حالة المستثمرين قليلي الخبرة. وهذا يعنى أن خبرة المستثمر كان لها تأثير معنوي على العلاقة محل الدراسة. ومن ثم تم **رفض فرض العدم، وقبول الفرض البديل.**

وتتفق هذه النتيجة مع دراسات (علي، 2019، موسى، 2018 ;Espahodi et al., 2019 Obamuyi, 2013; Christanti & Mahastanti, 2011) التي توصلت إلى وجود تأثير معنوي لمستوى الخبرة على قرار الاستثمار أو على العلاقة بين الإفصاح عن المعلومات غير المالية وقرار الاستثمار في الأسهم. **ويخلص الباحثان مما سبق،** إلى قبول الفرض الفرعي (H1a)، حيث يوجد تأثير معنوي لاختلاف خبرة المستثمر على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن

السيبراني وقرار الاستثمار بالأسهم. وتعكس هذه النتيجة ارتفاع الوعي بأهمية تأثير الأمن السيبراني على مستقبل الشركات من جانب المستثمرين ذوي الخبرة.

6-3-7-2-3 نتيجة اختبار الفرض الفرعي (H1b)

استهدف الفرض الفرعي (H1b) اختبار ما إذا كان مستوى التأهيل العلمي للمستثمر كمتغير معدل يؤثر معنويًا على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واستخدم الباحثان في هذا الشأن اختبار ويلكوكسون Wilcoxon Signed-Rank Test اللامعلمي لعينتين مرتبطتين (غير مستقلتين) لإجراء المقارنات الثنائية وتحديد مدى الاختلاف بين وسيطي العينتين. ولاختبار هذا الفرض تم تحويله الى صورة فرض العدم كما يلي:

H_0: لا يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى التأهيل العلمي للمستثمر.

ويتضح نتائج هذا الاختبار في الجدول رقم (9) على المقارنة الثالثة.

جدول 9: نتائج اختبار الفرض الفرعي (H1b)

	الفرض	الاختبار الاحصائي	الاختبار المستخدم	N	Z	P-value
H1b	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى التأهيل العلمي للمستثمر.	أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين المؤهلين علمياً.	Wilcoxon Signed Ranks Test	25	4.375	0.000
		أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين غير المؤهلين علمياً.		38	3.932	0.000

تشير نتائج الاختبار (جدول رقم 9) إلى أن كل من المستثمرين المؤهلين وغير المؤهلين علمياً يستجيبون بصورة معنوية للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني عند تقييم أسعار الأسهم واتخاذهم لقرار الاستثمار في الأسهم، حيث كانت قيمة (P-value) (.000) أقل من (5%). وهذا يعني أن مستوى التأهيل العلمي للمستثمر كان لها تأثير معنوي على العلاقة بين المحتوى المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

وقام الباحثان بإجراء مقارنة بين الحالات السابقة باستخدام قيمة(Z) المحسوبة، لتحديد مدى قوة تأثير مستوى التأهيل العلمي على العلاقة محل الدراسة، من خلال مقارنة قيمة(Z) المحسوبة في الحالة الأولي بالحالة الثانية، فكلما زادت قيمة(Z) المحسوبة، دل ذلك على قوة تأثير مستوى التأهيل العلمي

للمستثمر على العلاقة محل الدراسة. وبالرجوع إلى النتائج نلاحظ أن قيمة (Z) المحسوبة في حالة المستثمرين المؤهلين علمياً **أكبر من** قيمة (Z) المحسوبة في حالة المستثمرين غير المؤهلين علمياً. وهذا يعنى أن التأهيل العلمي للمستثمر كان لها تأثير معنوي على العلاقة محل الدراسة. ومن ثم تم **رفض فرض العدم، وقبول الفرض البديل.**

وتتفق هذه النتيجة مع دراسات (محمد، 2020، علي، 2019، موسى، 2018 ;Obamuyi, 2013 Miazee & Hasan, 2014; Rena et al, 2016; Hoang & Phang, 2021) التي توصلت إلى وجود تأثير معنوي لمستوى التأهيل العلمي على قرار الاستثمار أو على العلاقة بين الإفصاح عن المعلومات غير المالية وقرار الاستثمار في الأسهم. **ويخلص الباحثان مما سبق،** إلى قبول الفرض الفرعي (H1b)، حيث يوجد تأثير معنوي لاختلاف التأهيل العلمي للمستثمر على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بالأسهم. وتعكس هذه النتيجة أن التأهيل العلمي للمستثمرين يحسن من إدراكهم لتقرير إدارة مخاطر الأمن السيبراني، حيث إن المؤهلات والشهادات العلمية التي حصل عليها المستثمر لها تأثير معنوي على جودة أحكامه ومن ثم جودة قراره الاستثماري.

6-3-7-2-4 نتيجة اختبار الفرض الفرعي (H1c)

استهدف الفرض الفرعي (H1c) اختبار ما إذا كان كل من خبرة المستثمر ومستوى تأهيله العلمي كمتغيرين معدلين يؤثران معاً معنويًا على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار في الأسهم، واستخدم الباحثان في هذا الشأن اختبار ويلكوكسون Wilcoxon Signed-Rank Test اللامعلمى لعينتين مرتبطتين (غير مستقلتين) لإجراء المقارنات الثنائية وتحديد مدى الاختلاف بين وسيطي العينتين. ولاختبار هذا الفرض تم تحويله الى صورة فرض العدم كما يلي:

H_0: لا يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى الخبرة والتأهيل العلمي للمستثمر معاً.

ويتضح نتائج هذا الاختبار في الجدول رقم (10) على المقارنة الرابعة.

جدول 10: نتائج اختبار الفرض الفرعي (H1c)

الفرض		الاختبار الاحصائي	الاختبار المستخدم	N	Z	P-value
H1c	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى الخبرة والتأهيل العلمي للمستثمر معاً.	أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين ذوي الخبرة والمؤهلين علمياً.	Wilcoxon Signed Ranks Test	16	3.402	0.001
		أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار المستثمرين قليلي الخبرة وغير المؤهلين علمياً.		47	4.839	0.000

تشير نتائج الاختبار (جدول رقم 10) إلى أن كل من المستثمرين ذوي الخبرة والمؤهلين علمياً، وكذلك المستثمرين قليلي الخبرة وغير المؤهلين علمياً يستجيبون بصورة معنوية للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني عند تقييم أسعار الأسهم واتخاذهم لقرار الاستثمار في الأسهم، حيث كانت قيمة (P-value) (.001)، (.000) على الترتيب، أقل من (5%). وهذا يعني أن تفاعل الخبرة ومستوى التأهيل العلمي للمستثمر كان له تأثير معنوي على العلاقة بين المحتوى المعلوماتي لتقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

وقام الباحثان بإجراء مقارنة بين الحالات السابقة باستخدام قيمة(Z) المحسوبة، لتحديد مدى قوة تأثير تفاعل الخبرة ومستوى التأهيل العلمي على العلاقة محل الدراسة، من خلال مقارنة قيمة(Z) المحسوبة في الحالة الأولي بالحالة الثانية. وبالرجوع إلى النتائج نلاحظ أن قيمة (Z) المحسوبة في حالة المستثمرين ذوي الخبرة والمؤهلين علمياً **أقل من** قيمة (Z) المحسوبة في حالة المستثمرين قليلي الخبرة وغير المؤهلين علمياً. وهذا يعنى أن تفاعل الخبرة ومستوى التأهيل العلمي للمستثمر كان له تأثير معنوي على العلاقة محل الدراسة. ومن ثم تم **رفض فرض العدم، وقبول الفرض البديل.**

وتختلف هذه النتيجة مع دراسة محمد (2020) التي توصلت إلى عدم وجود تأثير معنوي لتفاعل الخبرة ومستوى التأهيل العلمي على قرار الاستثمار أو على العلاقة بين الإفصاح عن المعلومات غير المالية وقرار الاستثمار في الأسهم. **ويخلص الباحثان مما سبق**، إلى قبول الفرض الفرعي (H1c)، حيث يوجد تأثير معنوي لاختلاف مستوى الخبرة والتأهيل العلمي للمستثمر معاً على العلاقة الإيجابية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بالأسهم. وتعكس هذه النتيجة الوعي المرتفع للمستثمرين تجاه أهمية استثمار الشركة في الأمن السيبراني وحماية أمن المعلومات.

6-3-8 تحليلات أخرى (Other Analysis)

6-3-8-1 التحليل الإضافي

يعرف التحليل الإضافي Additional Analysis على أنه منهجية لإعادة اختبار العلاقات الرئيسية محل الدراسة بالتحليل الأساسي Fundamental Analysis، بعد تعديلها من خلال إدخال متغيرات جديدة ومعالجتها كمتغيرات رقابية أو معدلة، أو تغيير طريقة معالجة بعض المتغيرات، وذلك لإجراء مقارنة بين نتائج التحليلين الإضافي والأساسي، لتحديد مدى الاختلاف بينهما، وذلك بغرض توفير المزيد من الوضوح على العلاقات الرئيسية محل الدراسة بالتحليل الأساسي (زكي، 2018).

وفي ظل التحليل الإضافي قام الباحثان بتغيير معالجة المتغيرين المعدلين (الخبرة، مستوى التأهيل العلمي) **وتحويلهما إلى متغيرين رقابيين**، وبالتالي تم إعادة اختبار الفرضين الفرعيين (H1a, H1b) كل على حده، بالاعتماد على المدخل الرقابي، ومن ثم تم استبدال الفرضين الفرعيين، محل الدراسة، بسؤالين كما يلي:

س1: هل يؤثر مستوى خبرة المستثمر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية؟

س2: هل يؤثر مستوى التأهيل العلمي للمستثمر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية؟

وللإجابة على هذين السؤالين، قام الباحثان بتقسيم العينة فرعياً إلى عينتين مستقلتين، وتم استخدام اختبار مان ويتني Mann-Whitney Test لعينتين مستقلتين، وتوصل الباحثان إلى النتائج التالية في الجدول رقم (11):

جدول 11: نتائج الإجابة على (س1، س2)

معالجة المتغير	في ظل اعتبار خبرة المستثمر متغيراً رقابياً	في ظل اعتبار مستوى التأهيل العلمي للمستثمر متغيراً رقابياً	الاختبار المستخدم
P-value	0.038	0.010	Mann-Whitney Test

وبالنظر لقيمة P.Value نجدها (.038)، (.010) على التوالي، أي أقل من مستوى المعنوية (5%)، ومن ثم **تمت الاجابة على السؤالين (س1، س2)** "**بنعم**". وهذا يؤكد على أهمية هذين المتغيرين في التأثير على العلاقة محل الدراسة.

6-3-8-2 تحليل الحساسية

يُستخدم تحليل الحساسية Sensitivity Analysis كمنهجية أو أسلوب لتقييم قوة النتائج التي تم التوصل إليها من خلال التحليل الأساسي، وبيان مدى اختلاف افتراضاته عن نتائج التحليل الأساسي. وذلك من خلال اختلاف طرق قياس المتغيرات الرئيسية (التابع، المستقل) ويسمى One at a time Sensitivity Measures، أو اختلاف حجم العينة ويسمى بالتحليل العاملي Factorial Analysis، أو اختلاف الفترة الزمنية ويسمى بتحليل الحساسية التفاضليDifferential Sensitivity Analysis (زكي، 2018).

ويرى الباحثان أن ما يناسب البحث الحالي، هو إجراء تحليل الحساسية باختلاف طرق القياس لاختبار العلاقة الرئيسية للبحث في البيئة المصرية. لذلك فقد تم إعادة اختبار فرض البحث الرئيسي (H1) اعتماداً على طريقة قياس بديلة للمتغير التابع الخاص بقرار الاستثمار في الأسهم، حيث تم احتساب متوسط ردود عينة المستثمرين على الحالات الافتراضية باستخدام مقياس مكون من درجتين، يأخذ القيمة (1) في حالة موافق تمامًا، وموافق بدرجة كبيرة، والقيمة (صفر) في حالة موافق، وغير موافق إلى حد ما، وغير موافق تمامًا قياساً على (السيد، 2018؛ علي، 2019). ويعرض الجدول التالي رقم (12) نتائج اختبار الفرض الرئيسي للبحث في ظل تحليل الحساسية.

جدول 12: نتائج اختبار الفرض الرئيسي للبحث (H1) في ظل تحليل الحساسية

Test Statistics[a]	
	B_ - A
Z	-6.471[b]
Asymp. Sig. (2-tailed)	.000
a. Wilcoxon Signed Ranks Test	
b. Based on negative ranks.	

ويتضح من الجدول رقم (12) أن قيمة (P.Value) هي (.000) أقل من مستوى المعنوية (5%)، مما يعني رفض الفرض العدم وقبول الفرض البديل. **ومن ثم قبول الفرض الرئيسي H1 بنموذج تحليل الحساسية.** ويرى الباحثان أن هذه النتيجة تؤكد صحة ما توصلا إليه من نتائج في التحليل الأساسي.

6-3-9 خلاصة نتائج اختبار فروض البحث

يوضح الجدول التالي خلاصة نتيجة اختبار فروض البحث، على النحو التالي:

الفرض	صيغة الفرض	مدى التأييد في حالة التحليل الأساسي	مدى التأييد في حالة التحليل الإضافي	مدى التأييد في حالة تحليل الحساسية
الفرض الرئيسي H1	يؤثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني إيجابًا ومعنويًا على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.	تم قبوله	-	تم قبوله
الفرض الفرعي H1a	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى خبرة المستثمر.	تم قبوله	-	-
الفرض الفرعي H1b	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى التأهيل العلمي للمستثمر.	تم قبوله	-	-
الفرض الفرعي H1c	يختلف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى الخبرة والتأهيل العلمي للمستثمر معاً.	تم قبوله	-	-
السؤال الأول (س1)	هل يؤثر مستوى خبرة المستثمر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية؟	-	الإجابة بنعم	-
السؤال الثاني (س2)	هل يؤثر مستوى التأهيل العلمي للمستثمر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية؟	-	الإجابة بنعم	-

6-4 نتائج البحث والتوصيات ومجالات البحث المقترحة

يتناول هذا الجزء من البحث عرضاً لنتائج البحث، وتوصياته، ومجالات البحث المقترحة، وذلك على النحو التالي:

6-4-1 نتائج البحث

تناول البحث دراسة واختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. ويمكن عرض أهم نتائج البحث، بشقيه النظري والتجريبي على النحو التالي:

- فيما يتعلق بالشق النظري، خلص البحث إلى أن الأمن السيبراني، يشمل حماية الأنظمة والشبكات والبرامج وأصول المنشأة من الهجمات والحوادث الإلكترونية التي يمكن أن تؤثر على أداء عملها بشكل فعال وكفء، وذلك من أجل تحقيق أهداف الحفاظ على سرية المعلومات وسلامتها وتوافرها.
- كما خلص البحث في شقه النظري، إلى أن إدارة مخاطر الأمن السيبراني، يقصد بها قيام الشركات بتبني منهجية مناسبة تمكنها من تنفيذ وتشغيل ضوابط رقابية تساعدها على حماية أنظمتها وأصولها المعلوماتية. ولتحسين عملية إدارة هذه المخاطر، تحتاج الشركات إلى 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 على الشركة من الإدارة الفعالة لمخاطر الأمن السيبراني.
- كما خلص البحث في شقة النظري أيضًا، إلى أن هناك العديد من جهات وضع المعايير والجهات الرقابية والهيئات المنظمة لعمل البورصات في الدول المختلفة، اهتمت بتطوير وتنظيم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني من خلال إصدار العديد من الارشادات المهنية في هذا الصدد. الا أنه في مصر، وعلى الرغم من اهتمام مصر بالأمن السيبراني، الا أنه لم يتم إصدار ارشاد أو معيار ينظم عملية إعداد تقرير مخاطر الأمن السيبراني في مصر.
- وأيضًا خلص البحث في شقه النظري، إلى أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يرسل إشارات إيجابية عن الشركات للمستثمرين وغيرهم من أصحاب المصالح، حول الجهود المبذولة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية. وبالتالي يساهم في الحد من ظاهرة عدم تماثل المعلومات بين الإدارة وأصحاب المصالح، مما يُمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل. مما يُساعد في تحسين كفاءة قرارات الاستثمار التي يتم اتخاذُها. بالإضافة إلى أنه يوفر الثقة في أعمال الشركة،

وينعكس على الأداء المالي، وبالتالي يؤثر على سُمعة الشركة وأسعار الأسهم والتدفُّق النقدي المُستقبلي، مما ينعكس إيجاباً على تحسين الأداء المالي للشركات.

- كما خلص البحث في شقه النظري، إلى أن قرارات المستثمرين تعتمد في كثير من الأحيان على بعض سماتهم الشخصية وخصائصهم الفردية. حيث إن مستوى خبرة المستثمرين وتأهيلهم العلمي له تأثير على تحسين إدراكهم وفهمهم لمحتوى تقرير إدارة مخاطر الأمن السيبراني وغيره من المعلومات غير المالية التي تفصح عنها الشركات، مما يؤثر إيجابًا على تحسين جودة قرارهم الاستثماري.

- وقد خلص البحث في شقه التجريبي، إلى قبول الفرض الرئيسي للبحث (H1)، والمتعلق بوجود تأثير إيجابي ومعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم. وهو ما يتفق مع ما توصل إليه البحث في شقه النظري.

- وأيضاً خلص البحث في شقه التجريبي، إلى قبول الفرض الفرعي (H1a)، والمتعلق باختلاف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف مستوى خبرة المستثمر. وهو ما يتفق مع ما توصل إليه البحث في شقه النظري.

- كما خلص البحث في شقه التجريبي، إلى قبول الفرض الفرعي (H1b)، والمتعلق باختلاف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف مستوى التأهيل العلمي للمستثمر. وهو ما يتفق مع ما توصل إليه البحث في شقه النظري.

- كما خلص البحث في شقه التجريبي أيضًا، إلى قبول الفرض الفرعي (H1c)، والمتعلق باختلاف التأثير الإيجابي المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، باختلاف مستوى خبرة وتأهيل المستثمر معاً. وهو ما يتفق مع ما توصل إليه البحث في شقه النظري.

- **وفيما يتعلق بمدخل التحليل الإضافي**، فقد تم استبدال الفرضين الفرعيين (H1a, H1b) بسؤالين. استهدف السؤال الأول اختبار ما إذا كان مستوى خبرة المستثمر تؤثر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية محل الدراسة، وكانت الإجابة بنعم. واستهدف السؤال الثاني اختبار ما إذا كان مستوى التأهيل العلمي للمستثمر يؤثر على قرار الاستثمار في الأسهم، في سياق العلاقة التأثيرية محل الدراسة وكانت الإجابة أيضاً بنعم.

- **وفيما يتعلق بتحليل الحساسية في حالة الفرض الرئيسي H1**، تم التوصل إلى عدم اختلاف النتائج عن التحليل الأساسي، وأن نتائج اختبار الفرض في ظل التحليل الأساسي متينة Robust، ومن ثم قبول الفرض الرئيسي H1 بنموذج تحليل الحساسية.

6-4-2 توصيات البحث

وفقا لما انتهى اليه البحث من نتائج بشقيه النظري والتجريبي، وفي ضوء حدوده، يوصى الباحثان بما يلي:

- أهمية زيادة وعي الشركات والأجهزة الرقابية ذات الصلة، من خلال المؤتمرات والندوات العلمية، بأهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وتوكيد مراقب الحسابات على هذا الإفصاح.
- ضرورة قيام الجهات المصرية المعنية بإصدار معايير المحاسبة والمراجعة بتوفير إرشادات كافية عن محتوى تقرير إدارة مخاطر الأمن السيبراني، وأيضاً توفير إرشادات كافية عن مسئولية مراقب الحسابات عند التوكيد على إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني.
- ضرورة اهتمام الهيئة العامة للرقابة المالية بتوجيه وزيادة وعي الشركات بأهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، من خلال نشر ثقافة الإفصاح الاختياري عن هذه المعلومات في التقارير السنوية للشركات، عن طريق إصدار المعايير الإرشادية التي تنظم عملية إعداد وعرض تقرير مخاطر الأمن السيبراني والاستفادة من تجارب الدول الأخرى في هذا الشأن.
- يجب على الباحثين إجراء المزيد من الأبحاث في مجال الأمن السيبراني، ودراسة أثره على قرارات أصحاب المصالح من جهة، ومردود توكيد مراقب الحسابات على هذا الإفصاح على هذه القرارات من جهة اخرى.
- كما يوصى الباحث بضرورة اهتمام الجامعات المصرية خاصةً في مرحلة الدراسات العليا، بتدريس موضوعات عن الأمن السيبراني والثورة الصناعية الرابعة، وأهميتهما في توفير العديد من المعلومات التي تحسن من اتخاذ القرارات في الأجل الطويل من منظور محاسبي ومهني.

6-4-3 مجالات البحث المقترحة

يقترح الباحثان عددًا من مجالات البحوث المستقبلية والتي تُعد امتداداً لهذا البحث، وذلك على النحو التالي:

- أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على دقة توقعات المحللين الماليين.
- أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان: دراسة تجريبية.
- دراسة واختبار أثر مستوى الإفصاح عن مخاطر الأمن السيبراني على سمعة الشركة والأداء المالي للشركات.

- أثر توكيد مراقب الحسابات على إفصاح الشركات المقيدة بالبورصة المصرية عن تقرير إدارة مخاطر الأمن السيبراني على قراري الاستثمار ومنح الائتمان: دراسة تجريبية.
- أثر الخصائص التشغيلية للشركات على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وكفاءة الاستثمار: دراسة تجريبية.

المراجع

أولاً: المراجع باللغة العربية

الاستراتيجية الوطنية للأمن السيبراني، (2017-2021)، المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء، جمهورية مصر العربية، ص ص 1-19.

الدليل التنظيمي للأمن السيبراني، 2020، هيئة الاتصالات وتقنية المعلومات، السعودية، ص ص 1-54.

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

السيد، محمود محمد، ٢٠١٨، "**أثر درجة الملاءة المهنية لمنشأة مراقب الحسابات على جودة أحكامه المهنية بشأن أمور المراجعة الرئيسية والاستمرارية والمعلومات الأخرى في تقريره غير المعدل الجديد**"، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.

الهيئة الوطنية للأمن السيبراني، 2018، الضوابط الأساسية للأمن السيبراني، السعودية، ص ص 1-40.

تعليمات التكيف مع المخاطر السيبرانية، 2018، البنك المركزي الأردني، ص ص 1-32.

رميلي، سناء محمد رزق، 2020، أثر إفصاح الإدارة عن هيكل الرقابة الداخلية وتوكيد مراقب الحسابات عليه على قرارا الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية، **مجلة الإسكندرية للبحوث المحاسبية**، كلية التجارة، جامعة الإسكندرية، المجد 4، العدد الأول، ص ص 1-88.

شحاته، شحاته السيد، 2014، أثر توكيد مراقب الحسابات على إفصاح الشركات المقيدة بالبورصة عن مسئوليتها الاجتماعية على قراراي الاستثمار ومنح الائتمان: دراسة ميدانية وتجريبية، **مجلة**

المحاسبة والمراجعة، كلية التجارة، جامعة بني سويف، المجلد 2، العدد الأول، ص ص 127-185.

علي، صالح علي صالح، 2019، **إطار مقترح للتقرير عن الاستدامة وأثره على قرارات أصحاب المصالح بالتطبيق على الشركات الصغيرة والمتوسطة المقيدة ببورصة النيل المصرية**، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة بني سويف.

محمد، عمرو محمد خميس، 2020، أثر توكيد مراقب الحسابات على تقرير الأعمال المتكاملة على قرارا الاستثمار بالأسهم: دراسة تجريبية، **مجلة الإسكندرية للبحوث المحاسبية**، كلية التجارة، جامعة الإسكندرية، المجد 4، العدد الثالث، ص ص 1-105.

موسى، سعاد زغلول عبده، 2018، **أثر توكيد المراجع الخارجي على تقارير الأعمال المتكاملة على قراراي الاستثمار ومنح الائتمان: دراسة تجريبية**، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.

ثانياً: المراجع باللغة الأجنبية

Akisik, O., & Gal, G., 2020, Integrated reports, external assurance and financial performance, **Sustainability Accounting**, **Management and Policy Journal**, 11 (2): 317-350.

Ali, A., Lai, F., Brown, N., Lowry, P., and Ali, R., 2021, Stock market reactions to favorable and unfavorable information security events: A systematic literature review, **Computers & Security**, 110: 1-22.

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). 2017. Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program, AICPA Assurance Services Executive Committee, New York, NY.

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.

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

Brown, H., Cohen, J., and Zamora, V., 2018, CSR Disclosure Items Used as Fairness Heuristics in the Investment Decision, **Journal of Business Ethics**, 152 (1): 275-289.

Cheng, X. and Walton, S., 2019, Do Nonprofessional Investors Care About How and When Data Breaches are Disclosed?, **Journal of Information Systems**, 33 (3): 163-182.

Christanti N. and Mahastanti L., 2011, Faktor-Faktor Yang Dipertimbangkan Investor Dalam Melakukan Investasi, **Jurnal Manajemen Teori dan Terapan**, 4 (3): 37-51.

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.

Espahbodi, L., Reza, E., Juma, N., and Amy, W., 2019, Sustainability priorities, corporate strategy, and investor behavior, **Review of Financial Economics**, 37 (1): 149-167.

Frank, M., Grenier, J. and Pyzoha, J., 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.

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.

Hoang,H. & Phang, S., 2021, How does Combined Assurance Affect the Reliability of Integrated Reports and Investors' Judgments?, **European Accounting Review**, 30 (1): 175-195.

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.

Kelton, A. and Pennington, R., 2020, Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?, **Journal of Information Systems**, 34 (3): 133-157.

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.

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.

Landau, A., Rochell, J., Klein, C., Zwergel, B., (2020). Integrated reporting of environmental, social, and governance and financial data: Does the market value integrated reports? **Business Strategy and The Environment**, 29 (4): 1750-1763.

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

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

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.

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.

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.

Pavlopoulos, A., Magnis, C., and Iatridis, E., 2019, Integrated reporting: An accounting disclosure tool for high quality financial reporting, **Research in International Business and Finance**, 49: 13-40.

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.

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.

Reimsbach, D., Hahn, R., and Gurturk, A., 2018, Integrated reporting and assurance of sustainability information: An experimental study on professional investors' information processing, **European Accounting Review**, 27 (3): 559-581.

Rena, B., Gene, E., and Ozkull, F., 2016, The Impact of Opinions of the Independent Auditors on the Investor Decisions in Banking Sector: An Empirical Study on the Banks Operating in Turkey, **Accounting & Finance Research**, 5 (1).

SEC. 2011. Division of Corporation Finance. CF disclosure guidance: Topic No.2,Cybersecurity.https://www.sec.gov/divisions/corpfin/guidance/cfguidance-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.

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., 2021, Cyber-attacks and stock market activity, **International Review of Financial Analysis** 76: 1-15.

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 رقم (1) الدراسة التجريبية

جامعة بني سويف
كلية التجارة
قسم المحاسبة

الاستاذ الفاضل / الأستاذة الفاضلة

تحية طيبة وبعد....

في إطار قيام الباحثين بإعداد بحث، والذي يتعلق بموضوع:

" **أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم**"

ومقدم لسيادتكم القوائم المالية وتقرير إدارة مخاطر الأمن السيبراني للشركة (ص) التي تعمل في مجال الاستثمارات المالية وقائمة استقصاء المرفقة، لذا نرجو من سيادتكم التكرم باستيفاء بيانات هذه القائمة بكل وضوح، حيث يمثل ذلك جزء من متطلبات تحقيق الهدف من البحث، وتعد مشاركتكم هامة جدًا لأغراض الدراسة.

ونشكركم مقدمًا على حُسن تعاونكم، ونتمنى لكم مزيدًا من التقدم والرقي في حياتكم.

وتفضلوا بقبول فائق الاحترام والتقدير

الباحثان

أ.د/ محمود أحمد أحمد علي
أستاذ المحاسبة والمراجعة
كلية التجارة – جامعة بني سويف

د/ صالح علي صالح
مدرس المحاسبة والمراجعة
كلية التجارة – جامعة بني سويف

أولًا: بيانات عامة

1- المؤهل العلمي: .....

2- الوظيفة الحالية: .....

3- عدد سنوات خبرتك في وظيفتك الحالية: ..... سنة.

ثانيًا: أهم المصطلحات الفنية ذات صلة

- **الأمن السيبراني (Cybersecurity)** :هو مجموعة من التقنيات والعمليات التي تم تصميمها لحماية أجهزة الكمبيوتر والشبكات وقواعد البيانات والتطبيقات بما تحتويه من بيانات وما تقدمه من خدمات، من الهجمات الالكترونية (Cyberattacks) والوصول غير المصرح به، والتغيير، أو تعطيل، أو سوء استخدام، أو استغلال غير مشروع.
- **مخاطر الأمن السيبراني (Cybersecurity Risk)**، من أكبر المخاطر التي تواجهها الشركات، حيث يمكن لمخاطر الأمن السيبراني أن تؤدى الى ارتفاع التكاليف والتأثير السلبي على عوائد الشركات، والإضرار بقدرة الشركات على الابتكار واكتساب العملاء والحفاظ عليهم. كما أن الهجمات الإلكترونية مكلفة ولها تأثير واضح على المركز المالي للشركات. وقدم المعهد الأمريكي للمحاسبين القانونيين (2017) AICPA في أبريل 2017 إطارًا لإعداد تقرير إدارة مخاطر الأمن السيبراني لإرشاد الشركات ودعمها في الإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني.

ثالثًا: بيانات الدراسة التجريبية

الشركة (ص) شركة مساهمة مصرية تعمل في مجال الاستثمارات المالية، مدرجة في البورصة المصرية (EGX) منذ مايو 2005 وخاضعة للقانون 159لسنة 1981، وتقوم بإدارة محفظة استثمارية متنوعة في مجالات تكنولوجيا المعلومات، ومراكز البيانات، ومركز الاتصال، والمباني الذكية، والإلكترونيات الاستهلاكية، والأغذية والمشروبات، والنقل البري، والمدفوعات الإلكترونية. وتعمل الشركة على تمكين أكثر من14000 موظف ماهر، وتستوعب قاعدة عملاء دولية واسعة من العمليات التي تغطي مصر، المملكة العربية السعودية والإمارات العربية المتحدة وقطر، وبولندا وتنزانيا ونيجيريا. وفيما يلي القوائم المالية للشركة عن السنة المنتهية في 2020/12/31، والتي تم نشرها مرفقاً بها تقرير مراقب الحسابات في 2021/4/1.

1. قائمة المركز المالي المختصرة عن السنة المنتهية في 2020/12/31

بيان	2020	2019
إجمالي الأصول طويلة الأجل(1)	2.567.077.960	2.439.902.777
إجمالي الأصول المتداولة(2)	428.788.441	445.588.102
إجمالي الأصول ((1) + (2))	**2.995.866.401**	**2.885.490.789**
إجمالي حقوق الملكية (3)	1.021.057.835	1.185.511.638
إجمالي الالتزامات (4)	1.974.808.566	1.699.979.241
إجمالي حقوق الملكية والالتزامات (3) + (4)	**2.995.866.401**	**2.885.490.789**

2. قائمة الدخل المختصرة عن السنة المنتهية في 2020/12/31

بيان	2020	2019
إيراد النشاط	197.247.427	310.834.932
تكلفة النشاط	(89.647.674)	(86.200.775)
مجمل الربح	**107.599.753**	**224.634.157**
إيرادات تشغيل أخرى	-	179.119
مصروفات تشغيل	(223.228.549)	(165.458.783)
صافي الربح قبل الضريبة	**(115.628.796)**	**59.354.493**
ضريبة الدخل	599.360	(76.422)
صافي الربح بعد الضريبة	**(115.029.436)**	**59.278.071**
نصيب السهم في الأرباح	**(0.54)**	**0.25**

3. قائمة الدخل الشامل عن السنة المنتهية في 2020/12/31

بيان	2020	2019
صافي ربح العام	**(115.029.436)**	**59.278.071**
الدخل الشامل الآخر احتياطي تقييم استثمارات متاحة للبيع قبل الضرائب ضريبة الدخل المتعلقة بعناصر الدخل الشامل الأخرى	(4.178.749) 940.218	(4.666.200) 1.049.895
مجموع الدخل الشامل الآخر	(3.238.531)	(3.616.305)
إجمالي الدخل الشامل	**(118.267.967)**	**55.661.766**

4. قائمة التدفقات النقدية المختصرة عن السنة المنتهية في 2020/12/31

بيان	2020	2019
صافي التدفقات النقدية الناتجة من أنشطة التشغيل	459.468.682	342.267.476
صافي التدفقات النقدية الناتجة من الأنشطة الاستثمارية	(429.382.361)	(274.327.096)
صافي التدفقات النقدية الناتجة من الأنشطة التمويلية	(30.099.083)	(69.005.002)
رصيد النقدية وما في حكمها أول العام	404.546	1.469.168
رصيد النقدية وما في حكمها آخر العام	**391.784**	**404.546**

5. قائمة التغير في حقوق الملكية المتخصرة عن السنة المنتهية في 2020/12/31

بيان	2020	2019
رأس المال المصدر والمدفوع	1.071.997.595	1.071.997.595
احتياطات	105.466.346	104.945.103
أرباح مرحلة	(41.376.670)	4.563.608
توزيعات أرباح	-	(55.272.739)
صافي ربح العام	(115.029.436)	59.278.071
إجمالي حقوق الملكية	**1.021.057.835**	**1.185.511.638**

6- الإيضاحات المتممة عن السنة المنهية في 2020/12/31

أسس إعداد القوائم المالية: يتم إعداد القوائم المالية وفقاً لمعايير المحاسبة المصرية وفي ضوء القوانين واللوائح المصرية السارية وطبقًا لمبدأ التكلفة التاريخية، ويتم إعداد قائمة التدفقات النقدية طبقًا للطريقة غير المباشرة.

الحالة الأولى: في ضوء قراءتك للقوائم المالية السابقة وعلماً بأن تقرير مراجعة حسابات الشركة عن عام 2020 كان تقرير نظيف (غير متحفظ)، وبصفتك مستثمر هل توافق على ما يلي:

م	درجة الموافقة / العبارات	موافق تمامًا (5)	موافق بدرجة كبيرة (4)	موافق (3)	غير موافق إلى حد ما (2)	غير موافق تمامًا (1)
1	أنك سوف تستثمر في أسهم هذه الشركة					
2	إذا علمت أن سعر إقفال سهم الشركة في نهاية 2018، 2019، 2020 كان 0.53، 1.24 ، 0.73 على التوالي. فما توقعك لسعر السهم في نهاية 2021: أ-يثبت عند ..... جنيه ب- يزيد ليصبح ..... جنيه ج- يقل ليصبح ..... جنيه					

الحالة الثانية: افترض في الحالة السابقة، أن الشركة أعدت تقرير عن إدارة مخاطر الأمن السيبراني، وتم الإفصاح عنه ضمن مرفقات القوائم المالية لعام 2020. وظهر تقرير إدارة مخاطر الأمن السيبراني للشركة (ص) كما يلي:

تقرير إدارة مخاطر الأمن السيبراني للشركة (ص) لعام 2020

السادة/ مساهمي الشركة

قامت الشركة بالاستعانة بإطار اعداد 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 الالكترونية والوصول غير المصرح به، التي من الممكن أن تؤثر على أداء عملها بشكل فعال وكفء.

تم وضع وتصميم برنامج إدارة مخاطر الأمن السيبراني من خلال الخطوات التالية:

1- تم تحديد المخاطر الالكترونية التي من الممكن أن تتعرض لها الشركة.

2- تم تصميم وتفعيل هيكل رقابة للأمن السيبراني، لمعالجة المخاطر التي تم تحديدها في الخطوة الأولى ومتابعة خطط المعالجة.

3- تم اختبار الفعالية التشغيلية لضوابط رقابة الأمن السيبراني، ومدى فاعليتها في صد الهجمات الالكترونية.

4- يتم عمل تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني واتخاذ الإجراءات التصحيحية. ويشرف مجلس الإدارة على برنامج إدارة مخاطر الأمن السيبراني للشركة.

ولم تتعرض الشركة لأي هجمات الكترونية في السنة المالية المنتهية في 2020/12/31، وذلك بفضل فعالية برنامج الأمن السيبراني لديها، والذي تمكنت الشركة من خلاله تحقيق أهداف الأمن السيبراني المتمثلة في الحفاظ على سلامة وسرية وتوافر المعلومات.

التاريخ: 2021/4/1 **عضو مجلس الإدارة المنتدب**

أيمن البدوي

- **في ضوء قراءتك للقوائم المالية، وتقرير إدارة مخاطر الأمن السيبراني، وبصفتك مستثمر هل توافق على ما يلي:**

م	درجة الموافقة / العبارات	موافق تمامًا (5)	موافق بدرجة كبيرة (4)	موافق (3)	غير موافق إلى حد ما (2)	غير موافق تمامًا (1)
1	أن تقرير إدارة مخاطر الأمن السيبراني أثر على قرارك الذي اتخذته في الحالة الأولى.					
2	أن هذه الشركة ستكون لها الأولوية في الاستثمار في أسهمها مقارنة بالشركات المنافسة التي لم تنشر تقرير إدارة مخاطر الأمن السيبراني.					
3	إذا علمت أن سعر إقفال سهم الشركة في نهاية 2018، 2019، 2020 كان 0.53، 1.24 ، 0.73 على التوالي. فما توقعك لسعر السهم في نهاية 2021: أ-يثبت عند ..... جنيه ب- يزيد ليصبح ..... جنيه ج- يقل ليصبح ..... جنيه					