

تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره على أسعار الأسهم: دراسة تطبيقية علي الشركات المقيدة بالبورصة المصرية

د/ هبه بشير الطوخي عبد الفتاح

مدرس بقسم المحاسبة

كلية التجارة - جامعة بنها

Heba.abdefattah@fcom.bu.edu.eg

د/ سناء ماهر محمدي مسعود

أستاذ مساعد بقسم المحاسبة

كلية التجارة - جامعة بنها

sanaamaher13@yahoo.com

ملخص البحث

هدف البحث: تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره على أسعار الأسهم وذلك بالتطبيق علي الشركات المقيدة في البورصة المصرية.

التصميم والمنهجية: اعتمدت الدراسة علي مدخل تحليل المحتوى في فحص التقارير السنوية لعينة مكونة من (30) شركة مقيدة في البورصة المصرية خلال الفترة من عام (2020) حتى عام (2022)، بإجمالي مشاهدات (90) مشاهدة، لاختيار فروض البحث، وذلك باستخدام مجموعة من الأساليب الإحصائية.

النتائج والتوصيات: تشير نتائج هذا البحث إلي وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين كل من حجم مجلس الإدارة، واستقلال مجلس الإدارة، وتنوع مجلس الإدارة وبين مستوي الإفصاح عن مخاطر الأمن السيبراني، كما يوجد أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم (وهذا الأثر سلبي). **وإستناداً إلي ذلك يوصي الباحثان** بضرورة قيام الهيئات والمنظمات المهنية المسؤولة عن إصدار معايير المحاسبة المصرية بإصدار معيار محاسبي ينظم المحاسبة عن مخاطر الأمن السيبراني، مع الأخذ في الاعتبار تجارب الدول الأخرى التي ألزمت شركاتها بالإفصاح عن مخاطر الأمن السيبراني، بما يساهم في تحسين جودة الإفصاح، ومساعدة جميع أصحاب المصالح على تقييم مدى قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل.

الأصالة والإضافة: تقدم هذه الدراسة مساهمة وإضافة للأدب المحاسبي في هذا المجال من خلال تحليلها لأهم خصائص مجلس الإدارة التي تؤثر علي الإفصاح عن مخاطر الأمن السيبراني وانعكاس ذلك علي أسعار الأسهم في بيئة الأعمال المصرية، ومحاولة اقتراح مؤشر للإفصاح عن مخاطر الأمن السيبراني يتكون من (40) بند، ويمكن الاستعانة بهذا المؤشر كإرشادات في وضع معيار محاسبي شامل للإفصاح عن مخاطر الأمن السيبراني في البيئة المصرية كمثال لاقتصاديات الدول الناشئة.

الكلمات المفتاحية: خصائص مجلس الإدارة - مخاطر الأمن السيبراني - أسعار الأسهم.

Analyzing the Relationship between Board of Directors' Characteristics and Disclosure about Cybersecurity Risks and its Impact on Stock Prices: An Empirical Study on Companies Listed on The Egyptian Stock Exchange

Abstract

Research Purpose: The research aimed to analyze the relationship between board of directors characteristics and disclosure about cybersecurity risks and its impact on stock prices by applying it to companies listed on the Egyptian Stock Exchange.

Design and Methodology: The study relied on the content analysis approach to analyze the content of the annual reports for a sample of (30) companies listed on the Egyptian Stock Exchange during the period from (2020) to (2022), with a total (90) views, to test the research hypotheses using a set of statistical methods.

Results and Recommendations: The results of this research indicate that there is a positive and significant correlation between the size of the board of directors, the independence of the board of directors, and the diversity of the board of directors and the level of disclosure about Cybersecurity risks. There is also a significant effect for disclosure about Cybersecurity risks on Stock prices. (this effect is negative). **Based on this**, the researchers recommend the need for the professional bodies and organizations responsible for issuing Egyptian accounting standards to issue an accounting standard that regulates accounting for cybersecurity risks, taking into account the experiences of other countries that obligate their companies to disclose about Cybersecurity risks, which contributes to improve the quality of disclosure and helping all stakeholders to evaluate the company's ability to maintain information security and reduce the possibility of breaches and negative events in the future.

Originality and Value: This study provides a contribution and addition to the accounting literature in this field through analyzing the most important characteristics of the board of directors that affect on the disclosure about Cybersecurity risks and its reflection on stock prices in the Egyptian business environment, and an attempt to propose an index for the disclosure about Cybersecurity risks, which consists of (40) items, and this indicator can be used as guidance in developing a comprehensive accounting standard for disclosing cybersecurity risks in the Egyptian environment as an example for the economies of emerging countries.

Keywords: Board of Directors Characteristics – Cybersecurity risks – stock prices.

1- الإطار العام للبحث

1-1 المقدمة

أدى الاعتماد المتزايد للشركات في السنوات الأخيرة علي تطبيقات تكنولوجيا المعلومات وشبكات الإنترنت والحوسبة السحابية إلي زيادة تعرضها لحوادث الأمن السيبراني، الأمر الذي جعل الأمن السيبراني **Cyber Security** - الذي يتمثل في مجموعة من التقنيات والعمليات التي تم تصميمها لحماية الشبكات و أجهزة الكمبيوتر والبرامج وقواعد البيانات بما تحتويه من بيانات وما تقدمه من خدمات من الهجمات أو الأضرار أو الوصول غير المصرح به - مصدر قلق متزايد لدي الشركات في جميع أنحاء العالم ومصدر قلق لكافة الأطراف الداخلية بالشركة والأطراف ذات الصلة وخاصة المستثمرين (Gao et al., 2020)، حيث يترتب علي وقوع حوادث الأمن السيبراني العديد من الأضرار والخسائر التي قد تتحملها الشركات والتي قد تؤثر سلباً علي نموها وأدائها المستقبلي، لأسباب متنوعة أهمها: تعطيل العمليات، سرقة الأسرار التجارية والمعلومات، الإضرار بالسمعة وفقدان ثقة أصحاب المصالح، وانخفاض أسعار أسهم الشركة وقيمتها السوقية وحجم الاستثمارات، وانخفاض حجم المبيعات ومعدلات الائتمان، وفقدان الملكية الفكرية، ونكاليف التقاضي والغرامات، وانخفاض الإيرادات (Mattucci, 2023; Tosun, 2021). وبالتالي أصبحت المخاطر السيبرانية من أكبر التحديات التي تواجهها الشركات في السنوات الأخيرة، واستجابة لهذه التحديات المتزايدة أصبح مطلوباً من الشركات الإفصاح عن مخاطر الأمن السيبراني والجهود التي تبذلها الإدارة للحد من هذه المخاطر (Newman, 2018)، كما زاد طلب المستثمرين علي معلومات الأمن السيبراني للشركات باعتبارها أحد العوامل الرئيسية التي قد تؤثر علي قراراتهم الاستثمارية (Gao et al., 2020).

وفي ضوء ذلك، اتجهت العديد من المنظمات والهيئات المهنية بإصدار العديد من الارشادات لدعم الإفصاح عن مخاطر الأمن السيبراني وكيفية إدارتها (AICPA 2017; SEC, 2011, 2018)، والبحث عن آليات رقابية للحد من هذه المخاطر، وهو ما أدى إلي الاهتمام المتزايد بحوكمة الشركات لدورها الهام في إحكام الرقابة، ويُعد مجلس الإدارة أحد وأهم آليات حوكمة الشركات والتي تشمل الدور الإشرافي والرقابي المنوط به من قبل حملة الأسهم (Smali et al., 2022)، كما يقرر مجلس الإدارة السياسات المتبعة في الإفصاح الاختياري عن المخاطر التي قد تواجهها والتي من شأنها التأثير سلباً علي استمراريته، فالاعتماد علي وجود مجلس إدارة فعال يمكن أن يوازن بين عوائد الشركة ومخاطرها (Alkurdi et al., 2019)، ومن ثم فقد يلعب مجلس الإدارة دوراً مؤثراً في الإفصاح عن مخاطر الأمن السيبراني. وعلي ذلك تتضح أهمية البحث الحالي من خلال التعرف علي العلاقة بين خصائص مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم في بيئة الأعمال المصرية.

1-2 مشكلة البحث

أدى تطور تكنولوجيا المعلومات والاتصالات إلى إحداث تطور كبير في مجال المعلومات الذي صاحبه ظهور تهديدات سيبرانية كبيرة ومتنوعة تهدد أمن المعلومات وسلامة المعلومات التي تتضمنها، نظراً لأن هذا التطور التكنولوجي لم يصاحبه تطور مماثل في الإجراءات والضوابط الرقابية، كما لم يصاحبه تطور مماثل في وعي وخبرات العاملين ومستخدمي نظم المعلومات الإلكترونية (Al-Sartawi, 2020). كما زادت مخاطر الأمن السيبراني نتيجة انتشار فيروس كورونا (كوفيد-19) وتحول جميع الأعمال وبشكل مفاجئ إلى تطبيق أسلوب العمل عن بعد في ظل بيئة رقمية، والتي لم تكن بعض الشركات قد استعدت لها بشكل كافي (Sharton, 2020)، لذلك فرضت بيئة الأعمال العالمية اليوم على الشركات امتلاك بنية تحتية رقمية آمنة لإجراء معاملاتها التجارية، وتسمى هذه البنية التحتية الرقمية العالمية المترابطة بالفضاء السيبراني Cyberspace، والذي يشمل على الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والخدمات والمعلومات الرقمية (Kahyaoglu & Caliyurt, 2018).

وعليه أصبحت مخاطر الأمن السيبراني من أكبر التهديدات التي تواجه الشركات وتؤثر على مستقبلها، حيث يترتب على تلك المخاطر العديد من الآثار السلبية التي تبدأ من غرامات أو تكاليف تقاضي وقد تنتهي بفقد الشركة لسمعتها وفقد ثقة المساهمين وأصحاب المصالح فيها مما قد يؤثر على بقائها في السوق، (Kamiya et al., 2021)، فوفقاً لتقرير (CISCO, 2017) فإن أكثر من 20% من الشركات التي تتعرض لاختراق أمني تواجه خسائر كبيرة في الإيرادات وانخفاض في عدد عملائها وخسارة حصتها السوقية وانخفاض أسعار أسهمها، وقد بلغت إجمالي الخسائر حوالي 17 مليون دولار أمريكي لكل شركة، كما حدد تقرير (Kaspersky, 2018) أهم الدول العربية التي تعرضت لهجمات سيبرانية لأنظمتها وجاءت مصر في المركز الثالث بنسبة 57%. ونتيجة لذلك زادت الضغوط على الشركات بالإفصاح عن مخاطر الأمن السيبراني والجهود التي تبذلها للحد من تلك المخاطر (Newman, 2018)، وبذلك حظي الإفصاح عن مخاطر الأمن السيبراني باهتمام كبير من جانب أصحاب المصالح وخاصة المستثمرين كاستجابة لطلبهم للحصول على مزيد من المعلومات، لمساعدتهم في اتخاذ قراراتهم الاستثمارية (Li et al., 2018).

ومن ناحية أخرى، يُعد الإفصاح عن مخاطر الأمن السيبراني من أهم الوسائل لتحقيق الشفافية التي تتطلبها ممارسات حوكمة الشركات التي تسعى لها الأنظمة المختلفة، ويُعد مجلس الإدارة من أهم الآليات الهامة التي تساعد على تطبيق حوكمة الشركات بشكل فعال، فمجلس الإدارة هو المسئول عن إدارة أمور الشركة والقيام بأعمال الإشراف والتعيين والرقابة ورسم السياسات والأهداف ووضع الخطط الاستراتيجية والعمل على اتخاذ القرارات الاستثمارية بكل حيادية واستقلالية (Aguilar, 2014)، كما نص دليل حوكمة

الشركات في عام 2016 في الفقرة (4/2) أن "مجلس إدارة الشركة مسئول بشكل عام عن إدارة المخاطر علي النحو الذي يتفق مع طبيعة نشاط الشركة وحجمها والسوق التي تعمل بها، وللشركة تأسيس إدارة مستقلة للمخاطر طبقاً لاحتياجاتها، وتقع علي المجلس مسئولية وضع استراتيجية لتحديد المخاطر التي تواجه الشركة، وكيفية التعامل معها، ومستوي المخاطر التي تتعامل بها الشركة وعرض كل ذلك علي المساهمين بشكل واضح" (دليل حوكمة الشركات المصري، 2016). ومع زيادة الهجمات السيبرانية التي تتعرض لها الشركات أصبح الأمن السيبراني والمخاطر السيبرانية من أهم القضايا المطروحة علي مجلس الإدارة، ويُعد الإشراف الفعال من جانب مجلس الإدارة على جهود الإدارة لمعالجة هذه المشكلات أمرًا بالغ الأهمية لمنع الهجمات السيبرانية الناجحة والاستجابة لها بشكل فعال، وذلك لحماية الشركات وأصحاب المصالح، فضلاً عن حماية المستثمرين وسلامة أسواق رأس المال (Hartmann & Carmenate, 2021). وفي هذا الصدد أصدرت لجنة تداول الأوراق المالية الأمريكية إرشادات إضافية عام 2018 تؤكد التزامات الشركات بالإفصاح عن مخاطر الأمن السيبراني والانتهاكات المادية والتأثير المحتمل لهذه الانتهاكات على الأعمال والتمويل والعمليات، وتحث الشركات على الإفصاح عن إجراءات الأمن السيبراني ودور مجلس الإدارة ومشاركته في مراقبة المخاطر السيبرانية، وتشمل الإفصاحات علي ما إذا كان مجلس الإدارة هو المسئول بكامل هيئته علي مراقبة المخاطر، أو يتم تفويضها إلى بعض لجان مجلس الإدارة التابعة له، وما إذا كان الموظفون المسؤولون عن إدارة المخاطر يقدمون تقاريرهم إلى مجلس الإدارة (SEC, 2018).

وفي ذات السياق أشارت دراسة (Aguilar, 2014) أن مجالس الإدارة مسؤولة عن الإشراف على قيام الشركة بإنشاء برامج مناسبة لإدارة المخاطر والإشراف على كيفية تنفيذ الإدارة لتلك البرامج وتقديم المشورة للإدارة عند اتخاذ القرارات المتعلقة بالأمن السيبراني لحماية مصالح أصحاب المصلحة، في حين أشارت دراسة (Bujno et al., 2018) أن المجالس تشرف على عملية إدارة المخاطر من خلال إسناد مسؤوليات المخاطر إلى لجان مجلس الإدارة المختلفة ولجنة المراجعة. كما توصلت دراسة (Smaili et al., 2022) إلي أن فعالية مجلس الإدارة تؤثر بشكل إيجابي علي قرار الشركة بالإفصاح عن معلومات الأمن السيبراني، كما أن استقلال مجلس الإدارة والخبرة المالية لهما تأثير إيجابي علي الإفصاح عن مخاطر الأمن السيبراني، في حين أن حجم مجلس الإدارة ليس له أي تأثير علي هذا الإفصاح، بينما توصلت دراسة (Blonder, 2014) أن مجالس الإدارة لا تقضي وقتًا كافيًا أو تخصص موارد كافية للشركات لمعالجة قضايا الأمن السيبراني.، كما لم تتولى المجالس أنشطة الرقابة الرئيسية المتعلقة بالمخاطر السيبرانية.

ومن ناحية أخرى، أشارت دراسة (Li et al., 2018; Abdullah, 2019; Cheong et al., 2021) أن الإفصاح عن مخاطر الأمن السيبراني يساهم في تخفيض عدم تماثل المعلومات ويساعد أصحاب

المصالح علي تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، كما يُعد إحدى الطرق لزيادة المصداقية وحماية ومساعدة المستثمرين علي اتخاذ قراراتهم الاستثمارية مما ينعكس علي أسعار الأسهم، ويقلل من تكاليف التقاضي المحتملة التي قد تتعرض لها الشركات، ويزيد من الشفافية، ويساهم بشكل فعال في الحد من تشوهات الأسواق المالية وتحسين كفاءة الأسواق المالية وذلك بإرسال إشارات إيجابية إلي السوق بشأن الجهود المبذولة من قبل الشركة لتخفيض مخاطر الأمن السيبراني مما يؤثر إيجابياً علي أسعار الأسهم. في حين أشارت دراسة (الرشيدي، السيد، 2019، Kamuya et al., 2021; Mattucci, 2023; Tong, 2023) أن الإفصاح عن مخاطر الأمن السيبراني يؤثر سلباً علي أسعار الأسهم، حيث تمثل التغيرات الكبيرة والسلبية مؤشراً هاماً لرد فعل المستثمرين نتيجة ذلك الإفصاح والذي يؤثر علي قيمة الشركة، وعلي كفاءة السوق حيث إن المعلومات والأرباح والتدفقات النقدية المستقبلية التي تفصح عنها الشركة تنعكس علي الفور علي أسعار الأسهم. بينما توصلت دراسة (Juma'h & Alnsour, 2021) إلي عدم وجود تأثير جوهري بين الإفصاح عن خروقات الأمن السيبراني وأسعار الأسهم.

ونظراً لوجود تباين في نتائج الدراسات السابقة التي اهتمت بالعلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم، بالإضافة إلى ندرة الدراسات السابقة التي تناولت الموضوع في البيئة المصرية وبالتطبيق علي الشركات المسجلة في البورصة المصرية - في حدود علم الباحثان- كما أن معظم الدراسات تمت في بيئات أجنبية.

وفي ضوء ذلك يمكن صياغة مشكلة البحث في الإجابة على التساؤلات التالية:

- ما هي العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني في بيئة الأعمال المصرية؟
- ما هو أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم للشركات المسجلة في البورصة المصرية؟

1-3 أهداف البحث

يتمثل الهدف الرئيسي للبحث في تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم للشركات المسجلة بالبورصة المصرية، وينبثق عن هذا الهدف الأهداف الفرعية التالية:

- تحديد مدي تأثير خصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني.
- بيان أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم.

1-4 أهمية البحث

يستمد البحث أهميته من أهمية الموضوع الذي يتناوله، ومن ثم تتمثل أهمية البحث في:

أولاً: الأهمية العلمية

- تزايد الاهتمام بالإفصاح عن مخاطر الأمن السيبراني وذلك لما له من تأثير واضح علي أمن وسرية المعلومات ونجاح واستمرارية الشركات وتحسين جودة تقاريرها المالية، وزيادة اهتمام المجالس والهيئات والمنظمات المهنية بإصدار العديد من الإرشادات التي تنظم وتطور الإفصاح عن مخاطر الأمن السيبراني وكيفية وإدارتها، بهدف مساعدة أصحاب المصالح علي تقييم أداء الشركات في مجال الأمن السيبراني، والذي يعتبر من أهم الوسائل لتحقيق الشفافية التي تتطلبها ممارسات حوكمة الشركات وتخفيض عدم تماثل المعلومات.

- تُعد الدراسة الحالية امتداداً للأدبيات المحاسبية التي تناولت مجال الإفصاح عن مخاطر الأمن السيبراني، وذلك بالتركيز على دراسة العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم للشركات المسجلة بالبورصة المصرية، وهو ما قد يتسم بالندرة في الدراسات المحاسبية التطبيقية في البيئة المصرية في حدود علم الباحثان.

ثانياً: الأهمية العملية

- لقد حظى موضوع الإفصاح عن مخاطر الأمن السيبراني باهتمام كبير في الآونة الأخيرة بحكم ازدياد تطور تكنولوجيا المعلومات والاتصالات والتحول الرقمي، ومن ثم يحاول الباحثان تصميم مؤشر للإفصاح عن مخاطر الأمن السيبراني يتكون من (40) بند مشتق من الإصدارات والدراسات السابقة، ويتم قياس مستوى الإفصاح عن مخاطر الأمن السيبراني على أساس المحتوى المعلوماتي للمؤشر، وبالتالي تقديم دليل عملي على أهم خصائص مجلس الإدارة التي تؤثر في الإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم للشركات في بيئة الأعمال المصرية، وذلك من خلال بناء نموذجين متعددين المتغيرات تمثل فروض الدراسة، الأول لاختبار أثر خصائص مجلس الإدارة التي تؤثر في الإفصاح عن مخاطر الأمن السيبراني، والثاني لقياس أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم، من خلال إدخال متغيرات جديدة إلى النماذج التي سبق وقدمتها الدراسات السابقة مما يعكس مؤشرات جديدة ذات دلالة إحصائية في تفسير العلاقة التأثيرية بين المتغيرات البحثية المقترحة بالدراسة.

- نتائج الدراسة قد توفر معلومات هامة من شأنها مساعدة الجهات التنظيمية والمهنية في مصر على العمل على إصدار المعايير والتشريعات الملزمة والمنظمة لعمليات الإفصاح عن مخاطر الأمن السيبراني، كما تساهم في زيادة فهم وإدراك الشركات المصرية بأهمية الإفصاح عن مخاطر الأمن

السيبراني، كما تساهم في تمكين المستثمرين وأصحاب المصالح من تقييم مدى قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل مما يؤدي الي زيادة ثقتهم في الأداء المستقبلي للشركة وترشيد قراراتهم الاستثمارية.

1-5 منهج البحث

اعتمد الباحثان على المنهج الاستقرائي في مراجعة الأدب المحاسبي المتعلق بموضوع البحث بهدف الاستفادة منها في صياغة الإطار النظري، والمنهج الاستنباطي لاستكشاف وتفسير العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم. كما قام الباحثان بدراسة تطبيقية باستخدام أسلوب تحليل المحتوى في فحص التقارير السنوية لعينة من الشركات المسجلة في البورصة المصرية وذلك خلال الفترة من عام (2020) حتى عام (2022)، بغرض تطوير نماذج لقياس هذه العلاقات واختبار فروض البحث، وقد تم استخدام مصفوفة الارتباط ونموذج الانحدار في تفسير نتائج الدراسة التطبيقية.

1-6 حدود البحث

- يقتصر البحث علي تناول أثر خصائص مجلس الإدارة علي مستوى الإفصاح عن مخاطر الأمن السيبراني دون التطرق لباقي آليات حوكمة الشركات إلا في حدود ما يحقق هدف البحث.
- يقتصر البحث على اختبار أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم، دون التطرق لقياس الآثار الاقتصادية الأخرى لمستوى الإفصاح عن مخاطر الأمن السيبراني مثل: كفاءة الاستثمار، قيمة المنشأة، الأداء المالي للشركة، الاحتفاظ بالنقدية، تكلفة رأس المال، جودة أتعاب المراجعة.
- يقتصر البحث على استخدام مدخل تحليل المحتوى في فحص التقارير السنوية للشركات المسجلة بالبورصة المصرية والعاملة في قطاع البنوك، قطاع الخدمات المالية غير المصرفية، قطاع الاتصالات والاعلام وتكنولوجيا المعلومات، قطاع الخدمات والمنتجات الصناعية والسيارات، وقطاع الرعاية الصحية والأدوية. حيث أنها أكثر القطاعات المعرضة للتهديدات والحوادث السيبرانية، والمعلومات الحساسة التي تمتلكها هذه الشركات، وذلك خلال الفترة (2020 - 2022).

1-7 خطة البحث

انطلاقاً من أهمية البحث، وتحقيقاً لأهدافه والإجابة على تساؤلاته البحثية، فقد تم تقسيم الجزء المتبقي من البحث على النحو التالي: يعرض القسم الثاني: العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني، بينما يتناول القسم الثالث: أثر الإفصاح عن مخاطر الأمن

السيبراني علي أسعار الأسهم، كما يناقش القسم الرابع: الدراسات السابقة والفجوة البحثية وتطوير فروض البحث، ويعرض القسم الخامس: الدراسة التطبيقية، ويتناول القسم السادس: النتائج والتوصيات ومجالات البحث المستقبلية.

2- العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني

2-1 الإفصاح عن مخاطر الأمن السيبراني في الفكر المحاسبي

حظي الإفصاح عن معلومات المخاطر السيبرانية باهتمام واسع علي الصعيد المحلي والعالمي خلال الفترة الأخيرة، لاسيما مع توسع استخدام تكنولوجيا المعلومات والاتصالات والتحول الرقمي في كافة أنشطة معظم الشركات، فضلا عن الأهمية الجوهرية للمحتوي الإعلامي لهذه المعلومات في التأثير علي قيمة الشركة وكفاءة القرارات الاستثمارية، ويتناول الباحثان الإفصاح المحاسبي عن مخاطر الأمن السيبراني كما يلي:

2-1-1 الإفصاح عن مخاطر الأمن السيبراني والنظريات المفسرة له

يعرف الأمن السيبراني "Cyber Security" بأنه مجموعة من الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به (li et al., 2018). كما عرفه المعهد القومي للمعايير والتكنولوجيا (NIST,2018) بأنه عملية حماية المعلومات عن طريق منع الهجمات واكتشافها والتصدي لها، وكذلك منع سوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، لضمان توافرها وسلامتها ومصداقيتها وسريتها، وتأمين خصوصية البيانات. وعرفته (ISACA,2017) بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.

وفي نفس السياق أشارت دراسة (Al-Zyoud, 2020; Badawy, 2021) إلي أن الأمن السيبراني هو مفهوم شامل يشمل أمن المعلومات وضمان المعلومات، فهو يشمل كل التقنيات والعمليات والضوابط المصممة لحماية الأنظمة والشبكات والمعلومات من الهجمات السيبرانية وتقليل أو منع الأثار المالية المرتبطة بها، كما يقلل برنامج الأمن السيبراني الفعال من مخاطر الهجمات والحوادث الإلكترونية ويحمي الجميع من سوء الاستخدام أو الاستخدام غير المصرح به للأنظمة والشبكات والتقنيات ذات الصلة.

ويخلص الباحثان مما سبق أن الأمن السيبراني يتمثل في مجموعة من التقنيات والعمليات والوسائل التي تم تصميمها لحماية البرمجيات وأجهزة الكمبيوتر والأنظمة والشبكات وقواعد البيانات والمعلومات من مختلف الهجمات والاختراقات والتهديدات السيبرانية ومكافحتها والتقليل من اثارها، بهدف المحافظة علي سلامة ونزاهة الأصول المعلوماتية وحماية المجتمعات والمنظمات والأفراد من الوصول غير المصرح به للأنظمة والشبكات والتقنيات.

وفيما يتعلق بمخاطر الأمن السيبراني (Cybersecurity risk) فأنها تعتبر من أكبر المخاطر التي تواجهها الشركات ، فهي المخاطر التي تهدد عمليات الشركات بما فيها رسالة الشركة ورؤيتها أو سمعتها أو صورتها أو أصولها بسبب إمكانية الوصول غير المصرح به أو سوء الاستخدام أو التعطيل أو تدمير المعلومات (الهيئة الوطنية للأمن السيبراني ، 2018)، وأشارت دراسة كل من (Florakis et al., 2020; Badawy, 2021; Hartmann and Carmenate, 2021) إلي أن مخاطر الأمن السيبراني هي مجموعة المخاطر التكنولوجية والتنظيمية والتشغيلية علي أصول المعلومات والتكنولوجية التي تتعرض لها الشركات التي تعتمد علي تقنيات تكنولوجية المعلومات الحديثة، والتي قد تنتج عن اختراق نظام الأمن السيبراني لديها بما يحد من قدرته علي تحقيق أهدافه المرجوة، وبما يؤدي الي حدوث خسائر مالية أو تعطيل أو ضرر لسمعة الشركة.

وتنشأ مخاطر الأمن السيبراني نتيجة هجمات متعمدة أو أحداث غير متعمدة، وتأخذ هذه الهجمات العديد من الأنواع، كما في حالة الوصول غير المصرح به إلي الأنظمة الرقمية لأغراض سرقة الأصول المالية، والفكرية، والشخصية، وغيرها من المعلومات الحساسة بالشركات أو عملائها، أو شركاء الأعمال الآخرين، أو إفساد البيانات، أو تعطل أو التوقف عن ممارسة الأعمال، ويمكن أيضاً تنفيذ تلك الهجمات بالاعتماد علي هجمات الحرمان، التي تؤدي إلي رفض الخدمة علي مواقع الويب للشركة. وأيضاً قد يتم تنفيذ هذه الهجمات من أفراد من خارج الشركة أو من داخلها، لذا تتعرض الشركات إلي خسائر فادحة عند حدوث مثل هذه الهجمات (Dakin, 2012).

كما أشارت دراسة (Florakis et al., 2020; Kamiya et at., 2021) **إلي الآثار السلبية لمخاطر السيبرانية علي الشركات** حيث تؤدي إلي تلف أو فقد بعض المعلومات المالية للشركات مما تؤثر علي صافي أرباح الشركات، وتؤدي إلي زيادة التكاليف وتخفيض الإيرادات، وبالتالي قد يكون لها تأثير سلبي علي ثروة الملاك وسمعة الشركة واحتمال تعرضها للدعاوى القضائية وقرارات المستثمرين نتيجة التأثير السلبي علي أسعار أسهم الشركات وعلي تقييم أصحاب المصالح لقدرة الشركة علي الحفاظ علي أمن المعلومات، كما أنها قد تضر بقدرة الشركة علي الابتكار واكتساب العملاء والحفاظ عليهم ، وعلي

وضعها التنافسي في السوق. وهو الأمر الذي يشير الي ضرورة قيام الشركات بإدارة مخاطر الأمن السيبراني حتي يمكن تجنب آثارها السلبية.

وتأسيساً لما سبق فإن المخاطر السيبرانية تمثل أحد المخاطر المستحدثة في البيئة العالمية والمحلية وأن الشركات بحاجة إلي الإفصاح عن المخاطر السيبرانية التي تواجهها أو التي يتوقع أن تواجهها لتعزيز الإفصاح والشفافية في تقاريرها السنوية وبما يساهم في ترشيد القرارات الاستثمارية.

وفي هذا السياق، قدم الأدب المحاسبي العديد من النظريات التي تفسر دوافع الشركات للإفصاح عن المخاطر في تقاريرها السنوية (شرف، 2023؛ علي، علي، Hilary et al., 2016; Heroux 2022)، فترى نظرية الوكالة **Agency Theory** أن الشركات تميل إلي الإفصاح عن مزيد من المعلومات عن المخاطر السيبرانية من أجل تقليل تكاليف الوكالة وتقليل الصراعات بين الإدارة والمساهمين، وأن الإدارة تسعى بجانب تحقيق مصالحها إلي تعظيم مصالح المساهمين، كما يساعد هذا الإفصاح في تخفيض درجة عدم تماثل المعلومات المرتبطة بالأداء المستقبلي للشركات. في حين ترى نظرية الإشارة **Signaling Theory** أن الشركات تتجه إلي الإفصاح عن مخاطر الأمن السيبراني لإرسال إشارة إيجابية لأصحاب المصالح حول الجهود المبذولة من الشركة في التعامل مع المخاطر السيبرانية والحماية من الهجمات الإلكترونية وذلك للحد من عدم تماثل المعلومات بين الإدارة وأصحاب المصالح، ولتحسين سمعة الشركة، ولجذب المستثمرين، وزيادة قيمة الشركة، وطبقاً للنظرية الشرعية **Legitimacy Theory** فإن الشركات تميل الي الإفصاح عن المعلومات المتعلقة بالمخاطر والتهديدات المحتملة من أجل إضفاء الشرعية علي أنشطتها والحصول علي دعم قوي من المساهمين، لتجنب التقاضي وتكاليف السمعة وتقليل الحاجة إلي لوائح إضافية، لذلك فإن إضافة الشرعية علي أعمال الشركات يمكنها من إظهار قدرتها في إدارة المخاطر والتغلب عليها بكفاءة، ويعزز من ثقة المستثمرين ويجذب الموارد الحاسمة للشركة. بينما ترى نظرية أصحاب المصالح **Stakeholder Theory** أن الشركات عليها التزامات أخلاقية تجاه أصحاب المصالح، لذلك يجب عليها أن تقصح لهم عن المعلومات المتعلقة بالمخاطر السيبرانية حتي تساعدهم علي اتخاذ القرارات والحفاظ علي ثروتهم وهو ما ينعكس إيجابيا علي زيادة الثقة بين الشركة وأصحاب المصالح وتحسين سمعة الشركة.

وفي ضوء ما سبق يتضح للباحثان أنه بالرغم من تعدد النظريات المفسرة لدوافع الشركات للإفصاح عن المخاطر السيبرانية إلا أنها اجتمعت علي أهمية هذا الإفصاح ودوره في الحفاظ علي بقاء الشركة حيث يخفض من عدم تماثل المعلومات ويمكن المستثمرين وأصحاب المصالح من تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل مما يؤدي الي زيادة ثقتهم في الأداء المستقبلي للشركة وترشيد قراراتهم الاستثمارية.

2-1-2 جهود الهيئات والمنظمات المهنية في دعم الإفصاح عن مخاطر الأمن السيبراني

يُعد الإفصاح عن المخاطر السيبرانية أحد الاتجاهات الحديثة في الإفصاح عن المخاطر، نظراً لزيادة التهديدات التي تواجهها الشركات في الآونة الأخيرة، التي تعرض الشركات إلى خسائر مالية وتشغيلية وقانونية بالإضافة الي فقدان السمعة وثقة العملاء والمستثمرين، لذلك اتجهت الهيئات والمنظمات المهنية لإصدار العديد من الإرشادات التي تنظم وتطور الإفصاح الاختياري عن المخاطر السيبرانية وكيفية إدارتها، بهدف مساعدة أصحاب المصالح علي تقييم أداء الشركات في مجال الأمن السيبراني (Hilary et al., 2016) ، ومن أهم هذه الإصدارات ما يلي:

- لجنة تداول الأوراق المالية الأمريكية (SEC) Securities and Exchange Commission

فقد قامت عام 2011 بإصدار إرشادات حول الإفصاح عن المخاطر السيبرانية وما يجب أن تتخذه الشركات في الاعتبار عند تحليل المخاطر السيبرانية لأغراض الإفصاح عنها مراعاة ما يلي (SEC,2011): الحوادث السيبرانية السابقة وشدة وتواتر تلك الحوادث، احتمالية وقوع الحوادث السيبرانية والحجم الكمي والنوعي لهذه المخاطر والتكاليف المحتملة والأضرار الأخرى الناتجة عن اختلاس الأصول والمعلومات الحساسة وتلف البيانات، ومدى كفاية الإجراءات الوقائية المتخذة لتقليل تلك المخاطر. وفي عام 2018 أصدرت دليلاً إرشادياً للشركات المسجلة بالبورصة الأمريكية يتعلق بمتطلبات الإفصاح عن الأمن السيبراني، ويتكون الدليل من قسمين: القسم الأول يتناول طبيعة الأمن السيبراني وتعريفه ومخاطره وأثاره السلبية علي المستثمرين والشركات وأسواق المال وأهمية الإفصاح لأصحاب المصالح وأثارها علي الشركات وعملياتها، وإرشادات الإفصاح عن المخاطر السيبرانية وأهمية اتجاه الشركات للإفصاح والتوسع في متطلبات الإفصاح عن تلك الصادرة في عام 2011. ويتناول القسم الثاني مراجعة القواعد بشأن الإفصاح عن مشكلات الأمن السيبراني، متناولاً أهمية مراعاة كل من الأهمية النسبية وعوامل الخطر والموقف المالي والقانوني للشركة وطبيعة نشاطها والسياسات والإجراءات التي تتبعها الشركة لرقابة وإدارة المخاطر السيبرانية والإفصاح عن تعامل الشركة مع المخاطر السيبرانية في القوائم المالية أو في مناقشات وتحليلات الإدارة (SEC,2018). وفي عام 2022 أصدرت تعديلات علي قواعدها بشأن متطلبات الإفصاح عن إدارة المخاطر السيبرانية، متضمنة الإفصاح عن حوادث الأمن السيبراني غير الفردية غير الجوهرية والتي تصبح جوهرية في المجمل، وإعداد تقارير سنوية حول خبرة أعضاء مجلس الإدارة في مجال الأمن السيبراني إن وجدت، والإفصاح بشكل دوري عن الاستراتيجية والإجراءات والسياسات المتبعة في حوكمة المخاطر السيبرانية وتحديد المسؤول عن حوكمة الأمن السيبرانية (SEC. 2022).

- المعهد الأمريكي للمحاسبين القانونيين (AICP)، وضع في عام 2017 إطار متكامل لإعداد تقارير مخاطر الأمن السيبراني وطرق إدارتها بهدف دعم الشركات وإرشادها في الإفصاح عن مخاطر الأمن السيبراني، ويتكون الإطار من ثلاث أقسام رئيسية هي (AICPA, 2017): القسم الأول وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للشركة، وذلك لتوفير معلومات تمكن مستخدمي التقرير من فهم المخاطر السيبرانية للشركة وكيفية إدارتها لتلك المخاطر، ويتضمن هذا القسم علي تسعة عناصر هي: طبيعة أعمال الشركة وعملياتها، طبيعة المعلومات المعرضة للخطر، الأهداف الرئيسية لبرنامج إدارة مخاطر الأمن السيبراني المتعلقة بتوافر البيانات وسريتها وسلامتها، العوامل الي تؤثر علي المخاطر الحتمية للأمن السيبراني مثل التكنولوجيا المستخدمة وأنواع الاتصالات، هيكل حوكمة مخاطر الأمن السيبراني، عملية تقييم مخاطر الأمن السيبراني، اتصالات الامن السيبراني وجودة معلومات الأمن السيبراني، ضوابط الرقابة علي برنامج إدارة مخاطر الأمن السيبراني، عمليات مراقبة الأمن السيبراني. القسم الثاني: يتضمن تأكيد الإدارة بأن إعداد القسم الأول يتوافق مع المعايير التي وضعها المعهد الأمريكي للمحاسبين القانونيين، وتأكيد الإدارة علي فعالية أنظمة الرقابة علي المخاطر السيبرانية. القسم الثالث: يتضمن رأي مراقب الحسابات بشأن تقرير إدارة مخاطر الأمن السيبراني للشركة.

- معهد المحاسبين القانونيين الكندي (CPA- Canada (2017 بالتعاون مع هيئة سوق الأوراق المالية الكندية (CSA, 2017) فقد أصدروا إرشادات للشركات المقيدة بالبورصة بشأن كيفية الإفصاح عن مخاطر الأمن السيبراني، والإفصاح عن الآثار المحتملة للهجمات السيبرانية وأثرها علي الأداء المستقبلي للشركة، والإفصاح عن الحوكمة ودورها في الحد من تلك المخاطر.

- هيئة سوق المال السعودية، حيث أصدرت الدليل الاسترشادي للأمن السيبراني، والذي يهدف إلي إرساء الضوابط الخاصة بالأمن السيبراني في الشركات السعودية والتي تساعدهم علي تبني أفضل الممارسات الدولية والتشريعية بشأن إدارة مخاطر الأمن السيبراني (هيئة السوق المالية السعودية، 2019). كما أصدرت إطار تنظيمي للأمن السيبراني في قطاع الاتصالات وتكنولوجيا المعلومات في عام 2020 (الدليل التنظيمي للأمن السيبراني، 2020).

- وبشأن الإهتمام بمخاطر الأمن السيبراني في مصر، فقد تناول الدستور المصري عام 2014 في المادة (31) علي أن " الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه وعلي النحو الذي ينظمه القانون"، لذا تم إنشاء 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 البنية التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها، وتحقيق بيئة

رقمية آمنة في شتي المجالات. وتشمل الاستراتيجية علي التحديات والأخطار السيبرانية، وأهم القطاعات الحيوية المستهدفة، وعناصر خطورة التهديدات السيبرانية (الاستراتيجية الوطنية للأمن السيبراني 2017-2021). ثم صدر القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات لدعم منظومة مواجهة مخاطر الأمن السيبراني، ثم صدر قرار رئيس الوزراء رقم 276 في سنة 2020 الخاص بتعيين رئيس المكتب التنفيذي للمجلس الأعلى للأمن السيبراني ورئيس الأمانة الفنية.

ومما سبق يخلص الباحثان إلي تزايد اهتمام الهيئات والمنظمات المهنية في الدول المتقدمة بصور العديد من الإرشادات لدعم الإفصاح عن مخاطر الأمن السيبراني، بينما لم يحظى هذا الموضوع من الاهتمام في الدول النامية، لذلك يري الباحثان بضرورة إصدار معيار محاسبي مصري للإفصاح عن مخاطر الأمن السيبراني ينظم المعالجة المحاسبية ويلزم الشركات بالإفصاح عن مخاطر الأمن السيبراني بما يساهم في تحسين الشفافية وتوفير معلومات مفيدة لمتخذي القرارات.

2-2 أثر خصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني

يُعد مجلس الإدارة من أهم آليات حوكمة الشركات، ويمثل السلطة العليا التي تحكم وتدير الشركة بناءً علي تفويض من الجمعية العامة للمساهمين، فهو مسئول عن صياغة استراتيجية الشركة ومتابعة تنفيذها، بصورة تساعد علي تحقيق أهداف الشركة وتوفير الحماية اللازمة لأصحاب المصالح والحد من تضارب هذه المصالح، وذلك من خلال توجيه ورقابة الإدارة التنفيذية، كما يقرر مجلس الإدارة السياسات المتبعة في الإفصاح الاختياري عن المخاطر التي قد تواجهها والتي من شأنها التأثير سلباً علي استمراريته، فالاعتماد علي وجود مجلس إدارة فعال يمكن أن يوازن بين عوائد الشركة ومخاطرها (Alkurdi et al., 2019).

ومن ثم فقد يلعب مجلس الإدارة دوراً مؤثراً في الإفصاح عن مخاطر الأمن السيبراني، حيث أصبح الأمن السيبراني والمخاطر السيبرانية من أهم القضايا المطروحة علي مجلس الإدارة، فقد أدت انتهاكات البيانات والمخاطر الإلكترونية التي تعرضت لها الشركات في السنوات الأخيرة إلي تأثيرات سلبية علي أدائها المالي وسمعتها وفقد ثقة أصحاب المصالح فيها، وبالتالي أصبحت مخاطر الأمن السيبراني من أهم قضايا حوكمة الشركات بالنسبة لمجلس الإدارة حيث يتعين عليهم مساءلة المديرين التنفيذيين أو مواجهة التقاضي أو الخضوع للمراجعة من قبل المنظمين، وبالتالي أصبح مجلس الإدارة مكلف بالإشراف علي مخاطر الأمن السيبراني استجابة للتحديات الجديدة (Cossin & Lu, 2021).

وأدت المخاوف الواسعة الانتشار بشأن مخاطر الأمن السيبراني إلي زيادة اهتمام الهيئات والمنظمات المهنية بإصدار العديد من الإرشادات التي تنظم وتطور الإفصاح الاختياري عن مخاطر الأمن السيبراني، فقد قامت لجنة البورصة الأمريكية في فبراير 2018 بإصدار دليلاً يتضمن إرشادات للشركات الأمريكية

المسجلة تتعلق بمتطلبات الإفصاح عن الأمن السيبراني، وكان من ضمن هذه المتطلبات أن تقوم الشركات بالإفصاح عن طبيعة دور مجلس الإدارة في إدارة مخاطر الأمن السيبراني وبرنامج إدارة هذه المخاطر بالاشتراك مع إدارة الشركة والذي يكون له الأثر الإيجابي علي المستثمرين في قيام مجلس الإدارة بدوره كما يجب في هذه المسائل الهامة (SEC,2018). كما وضح الدليل الاسترشادي للأمن السيبراني الصادر عن هيئة سوق المال السعودي في عام 2019 أنه تقع كامل المسؤولية عن الأمن السيبراني علي عاتق مجلس الإدارة، وقد حدد مسؤوليات مجلس إدارة مؤسسة السوق عن الأمن السيبراني في الآتي (هيئة السوق المالية السعودية، 2019):

- تحديد الهيكل التنظيمي للأمن السيبراني والأدوار والمسؤوليات وتوثيقها وتنفيذها واعتمادها من قبل مجلس الإدارة.
 - التأكد من أن المعايير والإجراءات تعكس متطلبات الأمن السيبراني.
 - التأكد من قبول العاملين لسياسات الأمن السيبراني والالتزام بها، ودعم المعايير والإجراءات عند إصدارها وتحديثها.
 - التأكد من إدراج مسؤوليات الأمن السيبراني في الأوصاف الوظيفية للمناصب ذات العلاقة ووظائف الأمن السيبراني.
- كما يمكن لمجلس الإدارة تفويض صلاحيات الأمن السيبراني إلي لجنة معينة بالأمن السيبراني أو لجنة إشرافية، وتتضمن مسؤوليات لجنة الأمن السيبراني في تحديد حوكمة الأمن السيبراني ووضع استراتيجية الأمن السيبراني للشركة بالإضافة إلي تحديد سياسات الأمن السيبراني وضمان تنفيذ تلك السياسات.
- وفي ذات السياق قامت دراسة (Taylor & Maurer, 2021) بتقديم أدلة وقوائم مرجعية تساعد الإدارة العليا بتدابير قابلة للتنفيذ لتحسين الأمن السيبراني، وأشارت إلي أن مجلس الإدارة باعتباره أعلى مستوي قيادي في الشركة، فإنه يتحمل المسؤولية كاملة عن التحكم في المخاطر السيبرانية، وبالتالي يجب أن يشرف علي إستراتيجية الشركة وسياساتها والأنشطة في هذا المجال.

وحتى يستطيع مجلس الإدارة القيام بأداء مهامه بكفاءة وفعالية لابد أن تتوفر فيه مجموعة من الخصائص منها: **حجم مجلس الإدارة**، فيتسم حجم مجلس الإدارة الكبير بتنوع الخبرات واختلاف الآراء وهو ما يعزز من قوة الرقابة وسياسة الإفصاح بالشركة مما يكون له تأثير إيجابي علي كمية وجودة الإفصاح عن مخاطر الأمن السيبراني (Cossin & Lu, 2021)، وإن كان ذلك يتعارض مع نظرية الوكالة التي ترى أن المجالس الكبيرة قد تكون غير فعالة مقارنة بحجم المجالس الصغيرة (Saggar & Singh, 2017). **استقلال مجلس الإدارة**، ترى كل من نظرية الوكالة ونظرية أصحاب المصالح أن زيادة استقلال

مجلس الإدارة يساعد على خفض تكاليف الوكالة، كما يوفر حافزاً لمطالبة الإدارة العليا بتحسين شفافية الإفصاح عن المخاطر وذلك لتجنب مخاطر الإضرار بسمعتهم الشخصية (Heroux & Fortin, 2021). تنوع مجلس الإدارة، تري نظرية الإشارة أن تنوع مجلس الإدارة من حيث نوع الجنس، والعمر، والخبرة المهنية والتعليم والمهارات قد يكون حافزاً للإفصاح عن مخاطر الأمن السيبراني للحفاظ على سمعتها وتعزيز أدائها (Rrdu & Smaili, 2022). كما أن الفصل بين مناصبي رئيس مجلس الإدارة والمدير التنفيذي يخفض من الممارسات الانتهازية للإدارة ويدعم شفافية الإفصاح عن مخاطر الأمن السيبراني (cossin & Lu, 2021)، كما أن وجود لجنة علي مستوى مجلس الإدارة مسؤولة عن الأمن السيبراني مثل لجنة المراجعة أو لجنة المخاطر أو لجنة التقنية سيؤدي إلى قيادة الشركة للإفصاح عن المزيد من المعلومات المتعلقة بالأمن السيبراني (Lankton et al., 2021). كما تعتبر خبرة مجلس الإدارة في مجال تكنولوجيا المعلومات سمة ضرورية لمجلس الإدارة لأداء مسؤولياته الإشرافية على تكنولوجيا المعلومات، وخاصة تلك المتعلقة بمخاطر الأمن السيبراني (EY, 2020)، وتمكن مجلس الإدارة من تقديم المشورة والإشراف بشكل أفضل فيما يتعلق بإدارة مخاطر تكنولوجيا المعلومات (Vincent et al., 2019)، وفي ذات السياق أشارت دراسة (Heroux & Fortin, 2021) أن خبرة الأعضاء في مجال تكنولوجيا المعلومات تساعد المجالس علي أن تكون أكثر فاعلية في إعداد التقارير المالية المتعلقة بقرارات تكنولوجيا المعلومات من خلال تعزيز فهمهم لتأثير مخاطر تكنولوجيا المعلومات علي التقارير المالية ونطاق وأهمية انتهاكات البيانات واحتياجات معلومات الأمن السيبراني لأصحاب المصالح، وبالتالي فإن زيادة خبرة مجلس الإدارة في مجال تكنولوجيا المعلومات ستؤدي بالشركة إلى الإفصاح عن المزيد من المعلومات المتعلقة بمخاطر الأمن السيبراني.

3- أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم

حظي الإفصاح عن مخاطر الأمن السيبراني علي أهمية كبيرة في الأدب المحاسبي خلال الفترة الأخيرة، وذلك لما له من تأثير واضح علي أمن المعلومات ونجاح واستمرارية الشركات وتحسين جودة تقاريرها المالية (Yang et al., 2020). وفي هذا الصدد أشارت دراسة (Li et al., 2018) أن الإفصاح عن مخاطر الأمن السيبراني يساعد أصحاب المصالح علي تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل. كما أشارت دراسة (Abdullah, 2019) أن الإفصاح عن المخاطر يعد إحدى الطرق لزيادة المصداقية وحماية ومساعدة المستثمرين علي اتخاذ قراراتهم الاستثمارية مما ينعكس علي أسعار الأسهم، وفي نفس السياق أكدت دراسة (الصيرفي، 2018) علي أن الإفصاح عن المخاطر يعتبر عنصر رئيسي في حوكمة الشركات، حيث أن الإفصاح عن المخاطر يساعد في توفير معلومات مفيدة للمستثمرين ويؤثر علي قراراتهم، فالمستثمرين يتأثرون

مباشرة بالمعلومات الجديدة التي يتم توفيرها، مما ينعكس على أسعار الأسهم. كما يعكس التغيير في سعر السهم تقييم للتدفقات النقدية المستقبلية المتوقعة، كما أشارت دراسة (Du et al., 2016) إلي أنه كلما زادت المعلومات المفصح عنها كلما زادت أسعار الأسهم وينخفض التقلب في أسعار الأسهم وتقل مخاطر انهيار أسعار الأسهم. وأكدت دراسة (Cheong et al., 2021) أن الإفصاح عن مخاطر الأمن السيبراني يقلل من تكاليف التقاضي المحتملة التي قد تتعرض لها الشركات، ويزيد من الشفافية، ويساهم بشكل فعال في الحد من تشوهات الأسواق المالية وتحسين كفاءة الأسواق المالية وذلك بإرسال إشارات إيجابية إلي السوق بشأن الجهود المبذولة من قبل الشركة لتخفيض مخاطر الأمن السيبراني. وهذا ما يتفق مع نظرية الإشارة حيث تري أن الشركات تفصح عن مخاطر الأمن السيبراني لإرسال إشارة إيجابية إلي السوق عن مدي قدرتها علي التعامل مع مثل هذه المخاطر مما يزيد من ثقة المستثمرين في الشركة وينخفض مستوي عدم التأكد لديه بالتالي يؤثر علي قرار تداول المستثمر لأسهمه وحركة أسعار الأسهم.

ومن ناحية أخرى، أشارت دراسة (الرشيدى، السيد، 2019؛ Kamiya et al., 2021) إلي أن الإفصاح عن الهجمات والاختراقات السيبرانية يؤثر علي أسعار الأسهم وأحجام التداول حيث تمثل التغيرات الكبيرة والسلبية مؤشراً هاماً لرد فعل المستثمرين نتيجة ذلك الإفصاح والذي يؤثر علي قيمة الشركة، وعلي كفاءة السوق حيث أن المعلومات والأرباح والتدفقات النقدية المستقبلية التي تفصح عنها الشركة تنعكس علي الفور علي أسعار الأسهم، وبالتالي فإن الإفصاح عن الهجمات السيبرانية يمكن قياسه من خلال حجم التغيرات السلبية في أسعار الأسهم وحجم التداول خاصة بعد الإعلان عن الهجمات السيبرانية مباشرة.

ويخلص الباحثان مما سبق أن الإفصاح عن مخاطر الأمن السيبراني يساهم في تخفيض عدم تماثل المعلومات بين الشركة وأصحاب المصالح، وذلك عن طريق إرسال إشارات إيجابية إلي المستثمرين والأسواق حول مدي قدرة الشركة علي منع واكتشاف الانتهاكات السيبرانية وتصحيحها في حالة حدوثها، وذلك لكسب ثقتهم في أعمال الشركة وجذبهم وزيادة رغبتهم للاستثمار في الشركة، كما يقلل من تكاليف التقاضي المحتملة التي قد تتعرض لها الشركات، مما ينعكس علي الأداء المالي، وبالتالي يؤثر علي سمعة الشركة وأسعار الأسهم والتدفق النقدي المستقبلي.

4- الدراسات السابقة وتطوير فروض البحث

يقوم الباحثان في هذا القسم بتحليل أدبيات الفكر المحاسبي التي اهتمت بالعلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره على أسعار الأسهم، وذلك كمحاولة لتحديد الفجوة البحثية وتطوير فروض البحث، وفي إطار استكمال جهود تلك الدراسات سيتم تناولها كما يلي:

4-1 الدراسات التي اهتمت بأثر خصائص مجلس الإدارة علي الإفصاح عن مخاطر

الأمن السيبراني

استهدفت دراسة (Hsu & Wang, 2014) اختبار العلاقة بين خصائص مجلس الإدارة واحتمال حدوث انتهاكات لأمن المعلومات، وذلك بالتطبيق علي عينة من (1500) شركة مدرجة في مؤشر S&P بسوق الأوراق المالية بالولايات المتحدة الأمريكية، خلال الفترة 1997-2009، وقد توصلت الدراسة إلي أن المجالس الأكبر حجماً والمجالس ذات المديرين الأكبر سناً والمدة الأطول ترتبط سلباً باحتمالية حدوث انتهاكات أمنية، في حين أن المجالس التي بها نسبة مئوية أكبر من المستقلين ترتبط بشكل إيجابي مع احتمالية حدوث انتهاكات أمنية، ويرجع ذلك بأنهم يعتقدون أن المديرين الخارجيين قد لا يكون لديهم معرفة داخلية كافية بالشركة للمساهمة في تقليل احتمالية حدوث انتهاكات أمنية.

وتناولت دراسة (Higgs et al., 2016) فحص العلاقة بين لجان تكنولوجيا المعلومات على مستوى مجلس الإدارة واحتمال قيام الشركات بالإبلاغ عن الانتهاكات الأمنية، وذلك من خلال إجراء دراسة تطبيقية علي عينة من (362) شركة مدرجة بالبورصة الأمريكية، وباستخدام الخروقات الأمنية المبلغ عنها خلال الفترة 2005-2014، وقد أظهرت نتائج الدراسة أن الشركات التي لديها لجنة تكنولوجيا معلومات تابعة لمجلس الإدارة أكثر عرضة للإبلاغ عن الانتهاكات مقارنة بالشركات التي ليس لديها هذه اللجان، مما يعني أن لجان التكنولوجيا الأكثر رسوخاً تساعد في تخفيف أو منع الانتهاكات الأمنية، كما توصلت الدراسة إلي أن لجان مجلس إدارة تكنولوجيا المعلومات مرتبطة بشكل إيجابي بالكشف عن الانتهاكات الخارجية، وأن وجود هذه اللجنة يخفف من عوائد الأسهم السلبية غير الطبيعية الناشئة عن الانتهاكات الخارجية، بينما ترتبط لجان المخاطر والامتثال بشكل إيجابي بالكشف عن الانتهاكات الداخلية.

كما تناولت دراسة (Islam et al., 2018) اختبار أثر خصائص حوكمة الشركات (مجلس الإدارة، ولجنة المراجعة، ولجنة إدارة المخاطر) علي مدي انخراط الشركة بمراجعة الأمن السيبراني بواسطة المراجع الداخلي، وذلك من خلال إجراء دراسة ميدانية وتوزيع قائمة استبيان علي عينة مكونة من (970) مراجع داخلي، وقد توصلت الدراسة إلي أن التقييم الشامل للمخاطر الذي يقوم به المراجع الداخلي وكفاءاتهم بتقييم الحوكمة والرقابة وإدارة المخاطر السيبرانية لها تأثير إيجابي علي عملية مراجعة الأمن السيبراني، كما يوجد تأثير إيجابي لدعم مجلس الإدارة علي مراجعة الأمن السيبراني، في حين لا يوجد تأثير لكل من لجنة المراجعة والمديرين التنفيذيين للمراجعة الحاصلين علي الشهادات الأمنية.

استهدفت دراسة (Al- Sartawi, 2020) اختبار العلاقة بين حوكمة تكنولوجيا المعلومات والأمن السيبراني علي مستوي مجلس الإدارة للشركات المدرجة في بورصة الأوراق المالية لدول الشرق الأوسط

وشمال إفريقيا، وذلك من خلال إجراء دراسة تطبيقية علي عينة من (94) شركة خلال عام 2018، وقد أظهرت نتائج الدراسة وجود علاقة مهمة ومباشرة بين مجموعة التقنيات المتكاملة (IIG) ومستوي الأمن السيبراني للشركة، وهذا يشير إلي أهمية تعيين أعضاء مجلس الإدارة من ذوي المعرفة والخبرة في مجال تكنولوجيا المعلومات، مما يؤدي إلي قرارات أفضل يتخذها مجلس الإدارة عند مواجهة التهديدات والتحديات السيبرانية، بالإضافة إلي ذلك، يمكن أن تكون خبرة تكنولوجيا المعلومات في مجالس الإدارة مهمة لفهم ما يفعله رؤساء تكنولوجيا المعلومات في الداخل، وبالتالي يكون لدية فهم ودراية كافية لتحدي أفعالهم.

وتناولت دراسة (Lankton et al., 2021) انتهاكات الأمن السيبراني ودور حوكمة تكنولوجيا المعلومات في موثيق لجنة المراجعة للحد من انتهاكات الأمن السيبراني، وذلك من خلال دراسة تطبيقية علي عينة من (189) شركة، وقد أظهرت نتائج الدراسة أن تطبيق آليات حوكمة تكنولوجيا المعلومات يؤدي إلي الحد من مخاطر الأمن السيبراني، كما أن الشركات التي لديها لجنة تكنولوجيا للحماية من خرق البيانات هي التي تفصح عن أدوار مجموعة التقنيات المتكاملة (IIG) في ميثاق لجنة المراجعة، كما أن الشركات التي يشارك فيها مجلس الإدارة في حوكمة تكنولوجيا المعلومات تكون هي أكثر استعداداً للتعامل مع هذه المخاطر من خلال زيادة الاشراف علي أدوار مجموعة التقنيات المتكاملة (IIG).

استهدفت دراسة (Heroux & Fortin, 2021) اختبار العلاقة بين خصائص مجلس الإدارة والإفصاح عن الأمن السيبراني، من خلال دراسة تطبيقية علي عينة من (250) شركة مدرجة في المؤشر المركب S&P/TSX في بورصة الأوراق المالية تورنتو بكندا خلال عام 2018 باستخدام أسلوب تحليل الانحدار، وقد توصلت الدراسة إلي وجود علاقة إيجابية بين كلاً من وجود لجنة علي مستوي مجلس الإدارة مسؤولة عن الأمن السيبراني، وخبرة مجلس الإدارة في مجال تكنولوجيا المعلومات، واستقلال مجلس الإدارة، وتنوع مجلس الإدارة وبين الإفصاح عن الأمن السيبراني، بينما توجد علاقة سلبية بين طول مدة عضوية مجلس الإدارة والإفصاح عن الأمن السيبراني.

استهدفت دراسة (Radu & Smaili, 2022) اختبار أثر التنوع بين الجنسين في مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني، وذلك من خلال إجراء دراسة تطبيقية علي عينة مكونة من (60) شركة مدرجة في مؤشر (S&P/ TSX) ببورصة الأوراق المالية في كندا، خلال الفترة 2014-2018، وقد توصلت الدراسة إلي وجود علاقة إيجابية بين التنوع بين الجنسين في مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني، وان هذا التأثير الإيجابي يشترط وجود ثلاث أناث علي الأقل في مجلس الإدارة.

استهدفت دراسة (Smaili et al., 2022) اختبار تأثير فعالية مجلس الإدارة علي الإفصاح عن الأمن السيبراني، وذلك من خلال دراسة تطبيقية علي عينة مكونة من (300) شركة مدرجة في البورصة

الكندية علي مدار فترة خمس سنوات، وقد توصلت الدراسة إلي أن فعالية مجلس الإدارة تؤثر بشكل إيجابي علي قرار الشركة علي الإفصاح عن معلومات الأمن السيبراني، كما أن استقلال مجلس الإدارة والخبرة المالية لهما تأثير إيجابي علي الإفصاح عن مخاطر الأمن السيبراني، في حين أن حجم مجلس الإدارة ليس له أي تأثير علي هذا الإفصاح.

استهدفت دراسة (Remeis, 2023) دراسة كيفية تأثير التنوع بين الجنسين في مجالس الإدارة على الإفصاحات المتعلقة بالأمن السيبراني للشركات المخترقة في الولايات المتحدة، وتم جمع إفصاحات الأمن السيبراني يدويًا لـ 180 شركة مساهمة عامة تم الإبلاغ عن خرق سيبراني لها، كما تم جمع الإفصاحات للسنة التي سبقت حدوث الاحترق والسنة التي تليها، وقد أسفر ذلك عن عينة من 360 كشفًا عن مخاطر الأمن السيبراني، وقد توصلت الدراسة إلى أن الشركات التي تضم عددًا كبيرًا من النساء في مجالس إدارتها هي الأكثر احتمالية لنشر إفصاحات الأمن السيبراني.

4-2 الدراسات التي اهتمت بأثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار

الأسهم

استهدفت دراسة (Spanos&Angelis, 2016) اختبار أثر الإفصاح عن معلومات الأمن السيبراني علي أسعار الأسهم، وذلك من خلال إجراء دراسة نظرية تحليلية لعدد 45 دراسة، وقد توصلت الدراسة إلي اتفاق 75,5% من هذه الدراسات إلي وجود أثر إيجابي ومعنوي لإفصاح الشركات عن معلومات الأمن السيبراني علي أسعار الأسهم.

تناولت دراسة (Berkman et al., 2018) اختبار تأثير الوعي بالأمن السيبراني علي القيمة السوقية للشركات، وذلك من خلال دراسة تطبيقية علي عينة مكونة من (2264) شركة في أمريكا، بإجمالي مشاهدات (9677) مشاهدة، وقد توصلت الدراسة إلي وجود علاقة إيجابية بين الوعي بالأمن السيبراني والقيمة السوقية للشركة، فكلما زاد الوعي بالأمن السيبراني كلما قلت التهديدات الناشئة عن مخاطر الأمن السيبراني مما قد يؤدي إلي زيادة القيمة السوقية للشركة.

وحاولت دراسة (الرشيدي، السيد، 2019) اختبار أثر الإفصاح عن مخاطر الأمن السيبراني للشركات المقيدة بالبورصة المصرية علي أسعار الأسهم وأحجام التداول، وذلك من خلال إجراء دراسة مقارنة بين الشركات المصرية المسجلة في قطاع تكنولوجيا المعلومات وبين الشركات الأمريكية التي تعرضت لهجمات إلكترونية مؤخرًا وذلك خلال الفترة (2016-2017)، وقد أظهرت نتائج الدراسة ضعف الإفصاح عن مخاطر الأمن السيبراني في الشركات المصرية مقارنة بالشركات الأمريكية، كما توصلت إلي وجود أثر سلبي للهجمات الإلكترونية علي أسعار الأسهم وأحجام التداول.

كما حاولت دراسة (Kamiya et al., 2021) اختبار تأثير المخاطر السيبرانية علي سمعة الشركة وأسعار أسهمها، وذلك من خلال استخدام عينة مكونة من 244 شركة مقيدة بالبورصة الصينية والتي تعرضت لاختراق بياناتها، حيث تم جمع حوادث اختراق بيانات (6328 حادثة) وذلك خلال الفترة من عام 2005 إلى عام 2017، وقد توصلت الدراسة إلى أن المخاطر السيبرانية لها تأثير سلبي علي ثروة الملاك وسمعة الشركة نتيجة التأثير السلبي علي أسعار أسهمها، وتقييم الشركة من جانب أصحاب المصالح علي مقدرتها علي الحفاظ علي أمن المعلومات.

واستهدفت دراسة (Tuson, 2021) اختبار أثر الإفصاح عن تعرض الشركات للهجمات السيبرانية علي سمعة وقيمة الشركة في الأجل القصير والطويل، وذلك من خلال إجراء دراسة تطبيقية علي عينة من (169) شركة مقيدة في بورصة الأوراق المالية الأمريكية، وذلك خلال الفترة من عام 2004 حتى عام 2019، وقد توصلت الدراسة إلي أنه عندما تفصح الشركات عن تعرضها لهجوم سيبراني لأول مرة، يؤثر ذلك علي الشركة علي المدى القصير من خلال انخفاض العوائد اليومية وزيادة حجم التداول نتيجة ضغوط عمليات بيع أسهم الشركة، كما يوجد أثر علي المدى الطويل حتي خمس سنوات يتمثل في تأثير سياسات الشركة بسبب الأضرار السلبية علي سمعة وقيمة الشركة، حيث توجد علاقة سلبية بين الإفصاح عن الهجمات السيبرانية وسمعة وقيمة الشركة.

كما تناولت دراسة (Mattucci, 2023) اختبار أثر رد فعل السوق علي الإفصاح عن خروقات الأمن السيبراني، وتم دراسة أثر 778 حدثاً أمنياً حدثت بين الأعوام 2005 و 2021 في الولايات المتحدة الأمريكية، وقد توصلت الدراسة إلي أن الكشف عن خروقات الأمن السيبراني يؤدي إلى رد فعل سلبي كبير في السوق.

استهدفت دراسة (شرف، 2023) اختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، وذلك من خلال إجراء دراسة تجريبية علي عينة مكونة من (108) ممثلين في أعضاء هيئة التدريس وطلبة الدراسات العليا بكليات التجارة بالجامعات المصرية، كممثلين للمستثمرين غير المحترفين، وقد توصلت الدراسة إلي وجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين.

وحاولت دراسة (موسي، 2023) اختبار أثر العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتاع المراجعة، وذلك من خلال إجراء دراسة تجريبية علي عينة من مراجعي الحسابات بمكاتب المحاسبة والمراجعة المصرية وأعضاء هيئة التدريس ومعاونيهم بالجامعات المصرية، وقد توصلت الدراسة إلي وجود أثر إيجابي معنوي للإفصاح عن حوادث الأمن السيبراني علي أتاعاب المراجعة.

واستهدفت دراسة (موسي، وآخرون، 2023) إلى قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية علي قيمة المنشأة، وذلك من خلال إجراء دراسة تطبيقية على عينة مكونه من (8) بنوك و (6) شركات بقطاع الاتصالات والإعلام وتكنولوجيا المعلومات مقيدة بالبورصة المصرية، وبعدد (42) مشاهدة خلال الفترة (2019-2021)، وقد توصلت الدراسة إلى أن شركات العينة تصح عن المخاطر السيبرانية بمتوسط عام بلغ (24.35) وبنسبة إفصاح بلغت (46%)، ووجود علاقة ارتباط إيجابية معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشأة.

4-3 الفجوة البحثية

طبقاً لما انتهت إليه الدراسات السابقة يمكن الإشارة إلى أهم ما تتميز به الدراسة الحالية ومساهماتها في الأدب المحاسبي لتقليل الفجوة البحثية كما يلي:

1- اهتمت العديد من الدراسات بألية مجلس الإدارة كأداة هامة من أدوات حوكمة الشركات وبيان تأثيرها الفعال علي مستوي الإفصاح عن مخاطر الأمن السيبراني، إلا أن هناك تباين في نتائج هذه الدراسات، فتوصلت دراسة (Hsu & Wang, 2014) أن المجالس الأكبر حجماً والمجالس ذات المديرين الأكبر سناً والمدة الأطول ترتبط سلباً باحتمالية حدوث انتهاكات أمنية، في حين أن المجالس التي بها نسبة مئوية أكبر من المستقلين ترتبط بشكل إيجابي مع احتمالية حدوث انتهاكات أمنية. كما توصلت دراسة (Heroux & Fortin, 2021) إلى وجود علاقة إيجابية بين كل من وجود لجنة علي مستوي مجلس الإدارة مسؤولة عن الأمن السيبراني، وخبرة مجلس الإدارة في مجال تكنولوجيا المعلومات، واستقلال مجلس الإدارة، وتنوع مجلس الإدارة وبين الإفصاح عن الأمن السيبراني، بينما توجد علاقة سلبية بين طول مدة عضوية مجلس الإدارة والإفصاح عن الأمن السيبراني. في حين توصلت دراسة (Smaili et al., 2022) إلى أن استقلال مجلس الإدارة والخبرة المالية لهما تأثير إيجابي علي الإفصاح عن مخاطر الأمن السيبراني، في حين أن حجم مجلس الإدارة ليس له أي تأثير علي هذا الإفصاح. كما أنها لم تتناول بشكل كافي تحليل طبيعة العلاقة التأثيرية بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني، لذلك تحاول الدراسة الحالية تقديم دليلاً عملياً من البيئة المصرية حول أكثر هذه الخصائص تأثيراً علي الإفصاح عن مخاطر الأمن السيبراني في ضوء بعض النظريات التفسيرية التي استخدمت في هذا المجال، وبما يُساهم في تقليل الجدل والنقاش حول هذه العلاقة.

2- اقتصرت بعض الدراسات (Radu, & Smaili, 2022; Remeis, 2023) علي تناول أثر التنوع بين الجنسين في مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني، كما اقتصرت دراسة كل

من (Higgs et al., 2016; Al- Sartawi, 2020; Lankton et al., 2021) علي اختبار العلاقة بين حوكمة تكنولوجيا المعلومات والأمن السيبراني علي مستوي مجلس الإدارة وبالتركيز علي أثر خبرة مجلس الإدارة في مجال تكنولوجيا المعلومات علي الإفصاح عن الأمن السيبراني، دون التطرق إلي باقي خصائص مجلس الإدارة التي من الممكن أن يكون لها تأثير فعال علي مستوي الإفصاح عن مخاطر الأمن السيبراني، وهو ما يبرز أهمية الدراسة الحالية.

3- وجود تباين في نتائج الدراسات السابقة التي اهتمت بأثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم، فتوصلت دراسة (Spanos & Angelis, 2016) الي وجود علاقة إيجابية بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم، في حين توصلت دراسة كل من (الرشيدى، السيد، 2019، 2023; Mattucci, 2023; Kamiya et al., 2021) إلي وجود علاقة سلبية بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم، كما توصلت دراسات أخرى (موسى، وآخرون، 2023؛ Berkman et al., 2018) إلي وجود علاقة إيجابية بين الإفصاح عن المخاطر السيبرانية والقيمة السوقية للمنشأة، في حين توصلت دراسة (Tuson, 2021) إلي وجود علاقة سلبية بين الإفصاح عن الهجمات السيبرانية وسمعة وقيمة الشركة. لذلك تحاول الدراسة الحالية دراسة أثر خصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني وانعكاس ذلك علي أسعار الأسهم في البيئة المصرية وهو ما يميز الدراسة الحالية.

4- اقتصرت دراسة (موسى، 2023) علي دراسة أثر الإفصاح عن مخاطر الأمن السيبراني علي أتعاب المراجعة، دون التطرق إلي أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم في ضوء النظريات المفسرة لذلك، وهو ما يميز الدراسة الحالية.

5- ندرة الدراسات التي تناولت أثر خصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني وانعكاس ذلك علي أسعار الأسهم بالتطبيق على الشركات المسجلة في البورصة المصرية - في حدود علم الباحثان - كما أن غالبية الدراسات تمت في بيئات أجنبية، مما يتطلب أهمية اختبار هذه العلاقة التأثيرية في البيئة المصرية والتي تختلف في سماتها وخصائصها عن البيئات الأجنبية، لذلك تعد الدراسة الحالية امتداداً للدراسات السابقة وتتميز عنها بتحليلها بشكل متكامل للعلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم في البيئة المصرية كأحد الاقتصاديات الناشئة التي تحتاج إلي مزيد من الإفصاح والشفافية لجذب الاستثمارات.

6- تعتمد منهجية الدراسة الحالية على تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم على أسلوب تحليل المحتوى للتقارير المالية للشركات المسجلة

في البورصة المصرية والعاملة في القطاعات الأكثر تعرضاً للتهديدات والحوادث السيبرانية خلال الفترة من عام (2020) حتى عام (2022)، وهي بذلك تختلف عن دراسة كلاً من (Heroux & Fortin, 2021; Radu, & Smaili, 2022; Smaili et al., 2022; Spanos & Angelis, 2016; Kamiya et al., 2021)، حيث أن جميعها تمت في بيئات أجنبية.

4-4 تطوير فروض البحث

هدفت الدراسة إلي استكشاف أثر خصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني من ناحية، وتحليل أثر الإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم من ناحية أخرى، وفي ظل اختلاف نتائج الدراسات السابقة بشأن العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم، لذلك يحاول الباحثان الاستقادة من هذه النتائج ونظريات الأدب المحاسبي في تطوير فروض البحث كما يلي:

4-4-1 خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني

- حجم مجلس الإدارة

يلعب حجم مجلس الإدارة دوراً هاماً في زيادة فعالية المجلس في الرقابة والإشراف علي المديرين التنفيذيين، وطبقاً لنظرية الوكالة فإن مجالس الإدارة ذات الحجم الكبير تكون أقل احتمالاً للسيطرة عليها من قبل الإدارة، وتتميز بخبرة أوسع ومعرفة أكثر تنوعاً تمكنها من القيام بدورها الاستشاري وتوزيع عبء العمل ومهام اللجان بشكل أفضل (Hussainey & Al- Najjar, 2012) وهو ما يكون له أثر واضح علي تحسين مستوي شفافية وإفصاحات الشركات بما في ذلك الإفصاح عن مخاطر الأمن السيبراني، كما تري نظرية الاعتماد علي الموارد ونظرية أصحاب المصالح أن المجالس ذات الحجم الكبير تكون أكثر فعالية في اتخاذ القرارات التي تخدم الاحتياجات المتنوعة لأصحاب المصالح، مما يقلل من حالات عدم التأكد (Moumen et al., 2016).

وقد أشار دليل قواعد معايير حوكمة الشركات المصري الصادر عام 2011 إلي أنه يجب ألا يقل عدد أعضاء المجلس عن خمسة أعضاء، إلا أنه لم يحد الحد الأقصى لهذا العدد. كما أوضحت الدراسات السابقة نتائج متباينة تجاه العلاقة بين حجم مجلس الإدارة ومستوي الإفصاح عن المخاطر، فقد توصلت (Yaggar & Singh, 2017; Alkurdi et al., 2019) إلي أن حجم مجلس الإدارة الكبير له تأثير إيجابي علي إفصاح الشركة عن المخاطر، كما توصلت (Hsu & Wang, 2014) إلي أن المجالس الأكبر حجماً والمجالس ذات المديرين الأكبر سناً والمدة الأطول ترتبط باحتمالية أقل للانتهاكات الأمنية. في حين توصلت دراسة (Minnick & Schorno, 2018) إلي أن الشركات التي تعرضت لخرق لديها

مجالس إدارية أكبر مع خبرة مالية أقل، كما توصلت دراسة (Alzead, 2017; Ahmadi & Elbehi, 2018) إلي وجود علاقة سلبية بين حجم مجلس الإدارة ومستوي الإفصاح عن المخاطر، في حين توصلت دراسة (Smaili et al., 2022) إلي عدم وجود تأثير لحجم مجلس الإدارة علي مستوي الإفصاح عن مخاطر الأمن السيبراني.

ويتفق الباحثان مع تفسيرات العلاقة الإيجابية بين حجم مجلس الإدارة ومستوي الإفصاح عن المخاطر، حيث أن كبر حجم مجلس الإدارة يعزز من فعالية الدور الرقابي لمجلس الإدارة نظراً لتنوع الخبرة والمعرفة بين أعضائه، بما يسمح بتخصيص الواجبات بشكل أفضل وتقسيم المجلس إلي لجان متخصصة لمراقبة ومتابعة أعمال إدارة الشركة، بالإضافة إلي صعوبة سيطرة الإدارة علي المجالس الكبيرة، ومن ثم سوف تساعد علي الإفصاح عن المزيد عن المعلومات المتعلقة بالمخاطر. وبالتالي، فإنه يتوقع وجود علاقة إيجابية بين حجم مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني. وبناءً علي ذلك، يمكن صياغة الفرض الأول من البحث في صورة الفرض البديل علي النحو التالي:

توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين حجم مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني.

- استقلال مجلس الإدارة

يعتبر استقلال مجلس الإدارة من العناصر الهامة التي تحقق فعالية مجلس الإدارة عند القيام بمهامه الإشرافية والرقابية علي أعمال المديرين التنفيذيين والحد من قدرتهم علي التصرفات الانتهازية التي تخدم مصالحهم الشخصية دون الأخذ في الاعتبار مصالح الملاك (Lim, 2011)، وقد أيدت ذلك نظريات الأدب المحاسبي، حيث أشارت **نظرية الوكالة** إلي أن استقلال مجلس الإدارة يساعد علي تخفيض مشاكل الوكالة والحد من عدم تماثل المعلومات بين المديرين والمساهمين من خلال المزيد من الإفصاح (Khalil & Maghraby, 2017)، كما أشارت **نظرية أصحاب المصالح** إلي أن المديرين المستقلين لديهم وعي أكثر باحتياجات وتوقعات كافة أصحاب المصالح، وخاصة الحاجة إلي الإفصاح عن المزيد من المعلومات المرتبطة بالمخاطر (Elamer et al., 2019).

كما أكد الدليل المصري لقواعد حوكمة الشركات (الإصدار الثالث، 2016) علي زيادة نسبة الأعضاء المستقلين في مجالس إدارة الشركات مستهدفة في ذلك ضمان فعالية دور هذه المجالس في الرقابة علي أداء الشركات والتأكيد من اتخاذها القرارات التي تحقق المنافع لكافة أصحاب المصالح، حيث نص في الفقرة رقم (2-2-1) علي أن تكون أغلبية أعضاء المجلس من غير التنفيذيين بينهم عضوين مستقلين علي الأقل يتمتعون بمهارات فنية وتحليلية بما يعود بالنفع علي المجلس والشركة.

وقد أظهرت الدراسات السابقة نتائج متباينة تجاه العلاقة بين استقلال مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، فتوصلت دراسة (Heroux & Fortin, 2021; Smaili et al., 2022) إلى وجود علاقة إيجابية بين استقلال مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني، حيث قد تؤثر المجالس الأكثر استقلالية علي مستوي الإفصاح عن الأمن السيبراني من خلال مساعدة الإدارة في تحديد ما يحتاجه أصحاب المصالح المختلفون من معلومات متعلقة بالأمن السيبراني ومخاطره، وتقديم المشورة للإدارة وارشادها للخطط والقرارات الإستراتيجية لإدارة مخاطر الأمن السيبراني، بينما توصلت دراسة Hsu & Wang, 2014) إلى أن المجالس التي بها نسبة مئوية أكبر من المستقلين يرتبط أعضاء مجلس الإدارة بشكل إيجابي بحدوث الانتهاكات الأمنية، ويرجع ذلك إلي أن المديرين الخارجيين قد لا يكون لديهم معرفة داخلية كافية بالشركة للمساهمة في تقليل احتمالية حدوث انتهاكات أمنية، في حين توصلت Alzead, (2017) إلي وجود علاقة سلبية بين استقلال مجلس الإدارة والإفصاح عن المخاطر.

واستناداً إلي أن المديرين المستقلون هم أشخاص محترفون ليس لديهم دور إداري أو علاقة مع الشركة من خلال العمل أو الملكية ولديهم سمعة النزاهة المهنية، بالإضافة إلي أن وجود أعضاء مستقلون داخل مجلس الإدارة يساعد علي زيادة الدور الرقابي علي المديرين التنفيذيين ويحد من تعارض المصالح بين الإدارة والملاك، فقد يكون المديرون المستقلون أكثر ميلاً لتشجيع الشركات علي القيام بالمزيد من الإفصاح عن المعلومات المتعلقة بمخاطر الأمن السيبراني لأصحاب المصالح وخاصة المستثمرين. وبالتالي، فإنه يتوقع وجود علاقة إيجابية بين نسبة أعضاء مجلس الإدارة المستقلون ومستوي الإفصاح عن مخاطر الأمن السيبراني. وبناءً علي ذلك، يمكن صياغة الفرض الثاني من البحث في صورة الفرض البديل علي النحو التالي:

توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين استقلال مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني.

- تنوع مجلس الإدارة

يُعد تنوع مجلس الإدارة من إحدى الخصائص الهامة المرغوبة لهيكل مجلس الإدارة، ويرجع ذلك إلي أن تنوع المديرين من خلال توافر أعضاء إناث بالمجلس قد يعزز من فعالية المجلس ودوره الإشرافي والرقابي نتيجة التنوع في المهارات والخبرات والمعارف والقيم الأخلاقية وارتفاع جودة المناقشات والتشاور، مما يؤدي إلي تحسين جودة قرارات مجلس الإدارة بما يوفر الحماية لجميع أصحاب المصالح في الشركة (Martinez– Jimenez et al., 2020)، وهو ما أيدته نظريات الأدب المحاسبي، حيث أشارت نظرية الاعتماد علي الموارد إلي أن مشاركة الإناث في مجلس الإدارة سيؤدي إلي تنوع الأفكار والخبرات بما يؤدي إلي تحسين الدور الرقابي لمجلس الإدارة (Mustafa et al., 2017)، كما تفترض نظرية

التنشئة الإجتماعية بين الجنسين أن الإناث أكثر تحفظاً فيما يتعلق بالمخاطر كما أنهن أكثر التزاماً بالمعايير الأخلاقية (Kouaib & Almulhim, 2019)، كما أشارت نظرية الوكالة إلي أنه كلما كان مجلس الإدارة أكثر تنوعاً، كلما أدي ذلك إلي زيادة فعالية الرقابة التي يقوم بها، كما يؤدي تنوع مجلس الإدارة إلي زيادة استقلالية المجلس، وبالتالي تميل الشركات إلي الإفصاح عن المزيد من المعلومات لتخفيض تكاليف الوكالة والحد من عدم تماثل المعلومات بهدف حماية سمعة الشركة (Idan et al., 2021)، أما نظرية التطور الأخلاقي ونظرية الدور الاجتماعي تقترض أن تنوع مجلس الإدارة يمكن أن يُعزز عمق واتساع المناقشات والمداوات (الجوهرية، سليمان، 2021)، بالإضافة إلي أن الإناث تتبني معايير أخلاقية أعلى في قراراتهن وفي ممارسة سلطاتهن وبالتالي فإن وجود الإناث في مجلس الإدارة من شأنه أن يمنع محاولات الاحتيال بالشركة، ويحقق العديد من المنافع للمجلس ومن ثم للشركة وأصحاب المصالح (علي، عتس، 2021).

وقد أشار الدليل المصري لقواعد حوكمة الشركات (الإصدار الثالث، 2016)، علي أنه يجب مراعاة التنوع بين أعضاء مجلس الإدارة دون التحيز لجنس أو عقيدة، كما قامت الهيئة العامة للرقابة المالية بإصدار قراري رقم 123، 124 لسنة 2019 لضمان تمثيل العنصر النسائي في مجالس إدارات الشركات المقيدة بالبورصة المصرية (الهيئة العامة للرقابة المالية، 2019).

وبشأن العلاقة بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، فقد توصلت الدراسات إلي نتائج متباينة، فتوصلت دراسة (Radu & Smaili, 2022; Heroux & Fortin, 2021; Shukla & Pandey, 2023) إلي وجود علاقة ارتباط إيجابية بين تنوع مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني، حيث وجود نسبة كبيرة من المديرات الإناث في المجالس تقود الشركات إلي الإفصاح عن المزيد من المعلومات المتعلقة بالأمن السيبراني، بينما توصلت دراسة (AL – Yahyae et al., 2017) إلي وجود علاقة سلبية بين تنوع مجلس الإدارة والإفصاح عن المخاطر في التقارير المالية، في حين توصلت دراسة (علي، عتس، 2021) إلي عدم وجود تأثير لمشاركة المرأة سواء في مجلس الإدارة أو في لجنة المراجعة علي تفعيل دورهما في تحقيق أهداف حوكمة الشركات المصرية.

ورغم التباين في نتائج الدراسات التي تناولت العلاقة بين تنوع مجلس الإدارة ومستوي الإفصاح عن المخاطر، إلا أنه من المتوقع وجود علاقة إيجابية بين تنوع مجلس الإدارة من خلال نسبة الأعضاء الإناث بالمجلس ومستوي الإفصاح عن مخاطر الأمن السيبراني ويرجع ذلك إلي أن وجود الإناث بمجلس الإدارة قد يساعد علي زيادة فعالية المجلس وتحسين وظيفة وكفاءة اللجان المنبثقة منه، بما ينعكس علي تحسين جودة الإشراف علي القرارات الإدارية المتعلقة بمسائل الأمن السيبراني من خلال تنوع مستوي الخبرة، وأنماط الاتصال والإدراك، بالإضافة إلي أن الإناث لديهن معايير أخلاقية أعلى وأكثر نفوراً من المخاطر،

وأكثر التزاماً بحضور الاجتماعات بمعدلات أعلى من الذكور مما يؤدي إلي ارتفاع جودة المناقشات والتشاور وتقديم وجهات نظر مختلفة إلي مجلس الإدارة حول عوامل مخاطر الأمن السيبراني وأدوات التخفيف من مخاطر الأمن السيبراني، وهذا يؤدي إلي مزيد من الشفافية والإفصاح عن هذه المعلومات. وبناءً علي ذلك، يمكن صياغة الفرض الثالث من البحث في صورة الفرض البديل علي النحو التالي:

توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني.

4-4-2 العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم

من الناحية النظرية يؤدي المزيد من الإفصاح عن مخاطر الأمن السيبراني إلي الحد من ظاهرة عدم تماثل المعلومات بين الإدارة وأصحاب المصالح، عن طريق إرسال أشاره إيجابية لأصحاب المصالح والمستثمرين حول مدي قدرة الشركة علي منع واكتشاف الحوادث السيبرانية والحماية منها، مما يساعد المستثمرين علي تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، مما يساهم في تحسين كفاءة قراراتهم الاستثمارية، وبالتالي يؤثر علي سمعة الشركة وأسعار الأسهم والتدفق النقدي المستقبلي(علي، علي، 2022). وقد قدمت العديد من النظريات تفسيراً للعلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم (Heroux and Fortin., 2021; Kelton & Pennington, 2020؛ مراد، 2021؛ شرف، 2023 فطبقاً لنظرية الوكالة تري أن زيادة مستوي الإفصاح عن مخاطر الأمن السيبراني يخفض من تكاليف الوكالة ومن درجة عدم تماثل المعلومات بين الإدارة وأصحاب المصالح بما يسهم في عدم وجود ما يسمى بالمعلومات الخاصة التي تؤثر علي حجم التداول وقرارات المستثمرين والتغيير في أسعار الأسهم، وطبقاً لنظرية الإشارة فأنها تشجع الشركات علي أن تفصح عن مخاطر الأمن السيبراني لإرسال إشارة إيجابية إلي السوق عن مدي قدرة الشركة علي التعامل مع مثل هذه المخاطر مما يزيد من ثقة المستثمرين في الشركة وبالتالي يؤثر علي قرار تداول المستثمر لأسهمه وحركة أسعار الأسهم، ووفقاً لنظرية الشرعية فإنها تؤيد زيادة مستوي الإفصاح عن مخاطر الأمن السيبراني للحصول علي دعم قوي من المساهمين وبالتالي فإن رأي المستثمرين سيتأثر ومن ثم أسعار الأسهم وحجم التداول، وطبقاً لنظرية أصحاب المصالح فإنها تحت الشركات علي الإفصاح عن مخاطر الأمن السيبراني لأصحاب المصالح حتي تساعدهم علي الحفاظ علي ثروتهم مما يؤثر بالتبعية علي أسعار الأسهم.

ومن الناحية الأكاديمية فهناك جدل مستمر بشأن العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم، فقد توصلت بعض الدراسات (Gordon et al., 2010; Spanos & Angelis, 2016; Masuch et al., 2022) إلي وجود علاقة إيجابية معنوية بين الإفصاح عن معلومات الأمن

السيبراني وأسعار الأسهم، كما أكدت دراسة (Szubartowicz & Schryen, 2020) علي أن سعر السهم يتأثر بشكل إيجابي بإعلان الشركات عن استثماراتها في الأمن السيبراني، في حين توصلت دراسة (Goel & Shawky, 2014; kamiya et al., 2021)؛ الرشيدى، السيد، 2019 إلى وجود علاقة سلبية بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم، كما توصلت دراسة (Walton & cheng 2019) إلى وجود علاقة سلبية بين تعرض الشركات للهجمات الإلكترونية وقرار الاستثمار في أسهمها، كما وجدت دراسة (الصيرفي، 2018) تأثير سلبي معنوي لمستوي الإفصاح عن ممارسات إدارة المخاطر علي أسعار الأسهم، بينما توصلت دراسة (مراد، 2021) إلى عدم وجود علاقة معنوية بين مستوي الإفصاح عن المخاطر وتغير أسعار الأسهم. وفي ضوء الجدول السابق يمكن صياغة الفرض الرابع من البحث في صورة الفرض البديل علي النحو التالي:

يوجد أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني علي أسعار الأسهم.

5- الدراسة التطبيقية

يتناول هذا الجزء من البحث إجراء دراسة تطبيقية لاختبار فروض البحث باستخدام البيانات المنشورة للشركات المسجلة بالبورصة المصرية وذلك لقياس تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره على أسعار الأسهم باستخدام أسلوب المحتوى وتتمثل مقومات الدراسة التطبيقية لاختبار فروض البحث فيما يلي:

5-1 مجتمع وعينة الدراسة

يتمثل مجتمع الدراسة في مجموعة من الشركات المسجلة في بورصة الأوراق المالية المصرية والعاملة في قطاع البنوك، قطاع الخدمات المالية غير المصرفية، قطاع الاتصالات والإعلام وتكنولوجيا المعلومات، قطاع الخدمات والمنتجات الصناعية والسيارات، وقطاع الرعاية الصحية والأدوية. حيث أنها أكثر القطاعات المعرضة للتهديدات والحوادث السيبرانية، والمعلومات الحساسة التي تمتلكها هذه الشركات، وذلك خلال الفترة من عام 2020 إلى عام 2022، وقد تم تحديد العينة وفقاً للشروط التالية:

- أن تكون الشركة مقيدة في بورصة الأوراق المالية المصرية.
- توافر التقارير المالية السنوية وتقارير مجلس الإدارة وتقارير الاستدامة ونشرات الأعمال للشركة بانتظام خلال فترة الدراسة.
- أن تكون الشركة قد مضي على قيدها في البورصة أكثر من ثلاثة سنوات، وألا تكون قد تعرضت للشطب أو الاندماج أو التوقف خلال فترة الدراسة.

وقد نتج عن تطبيق الشروط السابقة اختيار (30) شركة تمثل عينة الدراسة بواقع (90) مشاهدة خلال فترة الدراسة. لتمثل عينة الدراسة موزعة على (5) قطاعات.

ويوضح جدول رقم (1) عدد شركات العينة والقطاع الذي تنتمي إليه ونسبة عدد شركات كل قطاع إلى إجمالي حجم العينة.

جدول 1: عدد ونسبة الشركات الممثلة لعينة الدراسة حسب القطاعات التي تنتمي إليها

م	اسم القطاع	عدد الشركات #	النسبة المئوية %
1	قطاع البنوك	6	20.0%
2	قطاع الاتصالات والإعلام وتكنولوجيا المعلومات	8	26.7%
3	قطاع الخدمات المالية غير المصرفية	7	23.3%
4	قطاع خدمات ومنتجات صناعية وسيارات	5	16.7%
5	قطاع الرعاية الصحية والأدوية	4	13.3%
	إجمالي عدد الشركات	30	100%

5-2 مصادر الحصول على البيانات

اعتمد الباحثان في جمع البيانات اللازمة للدراسة التطبيقية على تحليل القوائم والتقارير المالية للشركات محل الدراسة خلال الفترة من عام (2020) حتى عام (2022) والمنشورة في المواقع الإلكترونية للشركات، وموقع البورصة المصرية www.egx.com.eg، وموقع شركة مصر لنشر المعلومات www.egidegypt.com، وموقع معلومات مباشر www.mubasher.info.

5-3 توصيف وقياس متغيرات الدراسة

استناداً إلى فروض البحث، يمكن تحديد متغيرات الدراسة وتوصيفها وكيفية قياسها كما يلي:

5-3-1 المتغيرات المرتبطة بنموذج الدراسة الأول: أثر خصائص مجلس الإدارة على الإفصاح

عن مخاطر الأمن السيبراني

أولاً: المتغير التابع: الإفصاح عن مخاطر الأمن السيبراني

اعتمد الباحثان لقياس مستوى الإفصاح عن مخاطر الأمن السيبراني على بناء مؤشر (*) للإفصاح عن مخاطر الأمن السيبراني يتكون من (40) بنداً في (6) مجموعة لها أوزان ترجيحية متساوية (Equally weighted) وتم إعداد هذا المؤشر استناداً إلى المؤشر المستخدم في دراسة كل من (يعقوب،

(*) ملحق رقم (1) المؤشر المقترح للإفصاح عن مخاطر الأمن السيبراني.

وآخرون، 2022؛ شرف، 2023؛ موسي، وآخرون، 2023؛ Ramirez et al., 2023؛ Heroux Forting, 2021؛ (2022؛)، والذي يعتمد على جمع البيانات باستخدام تحليل المحتوى، كما تم الاعتماد على إصدارات الهيئات والمنظمات المهنية مثل: المعهد الأمريكي للمحاسبين القانونيين (AICP, 2017) ولجنة تداول الأوراق المالية الأمريكية (SEC, 2011؛ 2018)، ومعهد المحاسبين القانونيين الكندي (CPA-Canada (2017) وهيئة سوق الأوراق المالية الكندية (CSA, 2017)، والاستراتيجية الوطنية للأمن السيبراني (2017-2021) وذلك لمراعاة ظروف البيئة المصرية في المؤشر. وقد تم إعطاء متغير وهمي للبنود التي يحتويها المؤشر بحيث يتم إعطاء القيمة (1) للبنود الذي يتم الإفصاح عنه، و(صفر) للبنود الذي لا يتم الإفصاح عنه، ثم تجمع درجات كل شركة ونسبتها إلي الحد الأقصى للبنود الواجب الإفصاح عنها وهي (40) بند، ومن ثم يمكن حساب مستوي الإفصاح عن مخاطر الأمن السيبراني من خلال المعادلة التالية:

الإفصاح عن مخاطر الأمن السيبراني وفقاً للمؤشر المقترح

$$= \frac{\text{عدد البنود التي أفصحت عنها الشركة خلال الفترة}}{\text{إجمالي بنود المؤشر المقترح (40 بند)}} \times 100$$

ثانياً: المتغيرات المستقلة: خصائص مجلس الإدارة

ويمكن توضيح المتغيرات المستقلة من خلال نموذج الدراسة الأول، كما يتضح من الجدول التالي:

جدول 2: متغيرات نموذج الدراسة الأول وطريقة قياسها

العلاقة المتوقعة	طريقة القياس	الرمز	المتغيرات
أولاً: المتغير التابع			
	يقاس بنسبة الإفصاح عن مخاطر الأمن السيبراني وفقاً للمؤشر المقترح (قسمة عدد البنود التي أفصحت عنها الشركة خلال الفترة على إجمالي بنود المؤشر)	CRD	الإفصاح عن مخاطر الأمن السيبراني
ثانياً: المتغيرات المستقلة (خصائص مجلس الإدارة)			
+	عدد أعضاء مجلس الإدارة.	Bsize	حجم مجلس الإدارة
+	يقاس من خلال قسمة عدد الأعضاء غير التنفيذيين (المستقلين) على عدد أعضاء مجلس الإدارة.	BIND	استقلال مجلس الإدارة
+	يقاس من خلال قسمة عدد العضوات الإناث على عدد أعضاء مجلس الإدارة	Bdiv	تنوع مجلس الإدارة

5-3-2 المتغيرات المرتبطة بنموذج الدراسة الثاني: أثر الإفصاح عن مخاطر الأمن السيبراني

على أسعار الأسهم

أولاً: المتغير التابع: أسعار الأسهم

وتشير إلى السعر السوقي لسهم الشركة، وتم قياسه لأغراض التحليل الأساسي بسعر الإقفال للسهم في اليوم التالي لتاريخ تقرير مراقب الحسابات، أو أول جلسة تداول بعد تاريخ تقرير مراقب الحسابات، وذلك قياساً علي (Ge et al., 2010; Vazakidis et al., 2013; Nasution & Mita, 2017) الصيرفي، 2018)

ولأغراض تحليل الحساسية تم قياسه باستخدام التغير في سعر السهم، وهو عبارة عن الفرق بين سعر الإغلاق في سنة القياس والسنة السابقة لها، من خلال المقياس التالي:

سعر الإغلاق في سنة القياس - سعر الإغلاق في السنة السابقة / سعر الإغلاق في السنة السابقة، وذلك قياساً علي (Jizi & Dixon, 2016؛ الصيرفي، 2018).

ثانياً: المتغير المستقل: الإفصاح عن مخاطر الأمن السيبراني

ويتم قياسه من خلال نسبة الإفصاح عن مخاطر الأمن السيبراني وفقاً للمؤشر المقترح (قسمة عدد البنود التي أفصحت عنها الشركة خلال الفترة على إجمالي بنود المؤشر).

ثالثاً: المتغيرات الرقابية

قام الباحثان بإضافة بعض المتغيرات الرقابية إلى نموذج الدراسة والتي قد تؤثر على المتغير التابع (أسعار الأسهم)، وذلك بهدف ضبط العلاقة بين المتغير المستقل (الإفصاح عن مخاطر الأمن السيبراني) والمتغير التابع، كما يتضح من الجدول التالي:

جدول 3: متغيرات نموذج الدراسة الثاني وطريقة قياسها

العلاقة المتوقعة	طريقة القياس	الرمز	المتغيرات
	أولاً: المتغير التابع: أسعار الأسهم		
	وتشير إلى السعر السوقي لسهم الشركة، وتم قياسه لأغراض التحليل الأساسي بسعر الإقفال للسهم في اليوم التالي لتاريخ تقرير مراقب الحسابات، أو أول جلسة تداول بعد تاريخ تقرير مراقب الحسابات. ولأغراض تحليل الحساسية تم قياسه باستخدام التغير في سعر السهم، وهو عبارة عن الفرق بين سعر الإغلاق في سنة القياس والسنة السابقة لها، من خلال المقياس التالي: سعر الإغلاق في سنة القياس - سعر الإغلاق في السنة السابقة / سعر الإغلاق في السنة السابقة.	SP	أسعار الأسهم
ثانياً: المتغير المستقل: الإفصاح عن مخاطر الأمن السيبراني			
±	يقاس بنسبة الإفصاح عن مخاطر الأمن السيبراني وفقاً للمؤشر المقترح (قسمة عدد البنود التي أفصحت عنها الشركة خلال الفترة على إجمالي بنود المؤشر)	CRD	الإفصاح عن مخاطر الأمن السيبراني
ثالثاً: المتغيرات الرقابية			
+	اللوغار يتم الطبيعي لإجمالي الأصول في نهاية العام	SIZE	حجم الشركة
+	بقسمة صافي الربح بعد الضريبة على إجمالي الأصول في نهاية العام.	PROF	ربحية الشركة
-	قسمة إجمالي الالتزامات على إجمالي الأصول في نهاية العام	LEV	درجة الرفع المالي
+	متغير وهمي يأخذ (1) إذا تمت المراجعة في أحد المكاتب الكبرى أو (صفر) بخلاف ذلك	AUDIT	حجم مكتب المراجعة

4-5 نماذج الدراسة

سوف يتم استخدام تحليل الانحدار متعدد المتغيرات لاختبار فروض البحث وذلك على النحو التالي:

أولاً: النموذج الأول: أثر خصائص مجلس الإدارة على الإفصاح عن مخاطر الأمن السيبراني:

يستخدم هذا النموذج لاختبار الفرض الأول والثاني والثالث، والذي يختبر وجود علاقة ارتباط ذات دلالة معنوية بين الإفصاح عن مخاطر الأمن السيبراني كمتغير تابع وكل من: حجم مجلس الإدارة، استقلال مجلس الإدارة، تنوع مجلس الإدارة كمتغيرات مستقلة. ويأخذ النموذج المقترح الشكل التالي:

$$CRD = \beta_0 + \beta_1 BSIZE + \beta_2 BIND + \beta_3 BDIV + \varepsilon \quad (1)$$

حيث إن:

CRD: تشير إلى مستوى الإفصاح عن مخاطر الأمن السيبراني.

β_0 : ثابت نموذج الانحدار.

BSIZE: تشير إلى حجم مجلس الإدارة.

BIND: تشير إلى استقلال مجلس الإدارة.

BDIV: تشير إلى تنوع مجلس الإدارة.

ε : تشير إلى حد الخطأ العشوائي.

ثانياً: النموذج الثاني: أثر الإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم (في ظل

التحليل الأساسي)

يستخدم هذا النموذج لاختبار الفرض الرابع، والذي يختبر وجود أثر ذو دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني كمتغير مستقل على أسعار الأسهم كمتغير تابع، حجم الشركة، ربحية الشركة، درجة الرفع المالي، حجم مكتب المراجعة كمتغيرات رقابية.

ويأخذ النموذج المقترح الشكل التالي:

$$SP = \beta_0 + \beta_1 CRD + \beta_2 SIZE + \beta_3 PROF + \beta_4 LEV + \beta_5 AUDIT + \varepsilon \quad (2)$$

حيث أن:

SP: يشير إلى سعر الإقفال للسهم في اليوم التالي لتاريخ تقرير مراقب الحسابات.

β_0 : ثابت نموذج الانحدار.

CRD: تشير إلى مستوى الإفصاح عن مخاطر الأمن السيبراني.

SIZE: حجم الشركة.

PROF: ربحية الشركة.

LEV: درجة الرفع المالي.

AUDIT: حجم مكتب المراجعة.

ε : تشير إلى حد الخطأ العشوائي.

تحليل الحساسية: لإعادة اختبار الفرض الرابع

قام الباحثان بإجراء تحليل الحساسية من خلال تغيير طريقة القياس، وتحديد طريقة قياس المتغير التابع والمتعلق بأسعار الأسهم، وذلك باستخدام التغير في سعر السهم، والذي تم قياسه وفقاً للتحليل الأساسي بسعر الإقفال للسهم في اليوم التالي لتاريخ تقرير مراقب الحسابات، وذلك لتوضيح أي من طرق القياس أفضل للتحقق من العلاقات محل الدراسة في بيئة الأعمال المصرية، وذلك قياساً على (Jizi & Dixon, 2016؛ الصيرفي، 2018)، حيث تم إعادة تشغيل النموذج المستخدم لاختبار فرض البحث الرابع، والذي يتعلق باختبار أثر الإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم.

وتم إجراء تحليل الحساسية بالاعتماد على نفس نموذج الانحدار السابق رقم (2) لاختبار فرض البحث الرابع، وفيما يلي توضيح لهذا النموذج:

$$SP = \beta_0 + \beta_1CRD + \beta_2SIZE + \beta_3PROF + \beta_4LEV + \beta_5AUDIT + \varepsilon \quad (3)$$

حيث أن:

SP: التغير في سعر السهم، وهو عبارة عن الفرق بين سعر الإغلاق في سنة القياس والسنة السابقة لها علي سعر الإغلاق في السنة السابقة.
وباقى المتغيرات كما سبق تعريفها.

5-5 الأساليب الإحصائية المستخدمة لاختبار فروض البحث

استخدم الباحثان أسلوب تحليل الانحدار متعدد المتغيرات لاختبار فروض البحث، حيث استخدم نموذجان انحدار لاختبار فروض البحث والتي سبق عرضهما. كما تم تحديد مستوى المعنوية *Significance level* المقبول على أنه يساوي (0.05) أو أقل. ولتقدير هذه النماذج تم استخدام برنامج (SPSS) الإصدار (26)، وبرنامج تحليل مشاهدات الاقتصاد القياسي (E-Views) الإصدار (11)، وللذان يعتبران من أهم البرامج المناسبة والأكثر استخداماً في مثل هذه الدراسات.

5-6 نتائج الدراسة التطبيقية

في ضوء فروض الدراسة، وبناءً عن نتائج التحليل الإحصائي التي تم التوصل إليها في هذه الدراسة، سوف يتم عرض النتائج وتفسيرها، وذلك على النحو التالي:

5-6-1 اختبار صلاحية البيانات للتحليل الإحصائي

للتحقق من صلاحية بيانات الدراسة للتحليل الإحصائي وتقدير نماذج الدراسة تم إجراء الاختبارات التالية:

5-6-1-1 اختبار اعتدالية المتغيرات *Test of Normality*

قام الباحثان باستخدام اختبار *Kolmogorov-Smirnov* للتحقق من مدى تبعية بيانات متغيرات الدراسة للتوزيع الطبيعي، بحيث أنه إذا كانت قيمة (*Sig.*) لمتغير ما أكبر من (0.05)، فإن هذا يدل على أن بيانات المتغير تتوزع توزيعاً طبيعياً، أما إذا كانت أقل من (0.05)، فإن هذا يدل على أن بيانات المتغير لا تتوزع توزيعاً طبيعياً (أمين، 2013). والجدول رقم (4) يوضح نتائج اختبار التوزيع الطبيعي لمتغيرات الدراسة.

جدول 4: نتائج اختبار *Kolmogorov-Smirnov* لاختبار اعتدالية متغيرات الدراسة

النموذج الثاني (تحليل الحساسية)			النموذج الثاني (التحليل الأساسي)			النموذج الأول			المتغيرات
<i>Sig.</i>	<i>Df</i>	<i>Statistic</i>	<i>Sig.</i>	<i>df</i>	<i>Statistic</i>	<i>Sig.</i>	<i>df</i>	<i>Statistic</i>	
0.089	90	0.414*	0.089	90	0.414*	0.196	90	0.140*	CRD
						0.278	90	0.099*	Bsize
						0.099	90	0.303*	BIND
						0.197	90	0.142*	Bdiv
0.082	90	0.474*	0.080	90	0.519*				SP
0.091	90	0.336*	0.091	90	0.336*				SIZE
0.136	90	0.297*	0.136	90	0.297*				PROF
0.297	90	0.084*	0.297	90	0.084*				LEV
0.088	90	0.420*	0.086	90	0.435*				AUDIT

- المصدر: (الجدول من إعداد الباحثان من واقع نتائج التحليل الإحصائي).
 - * العلاقة ذات دلالة إحصائية عند مستوى معنوية (0.05) أو أقل.

يتضح من الجدول رقم (4) أن القيمة المعنوية (*Sig.*) لجميع متغيرات الدراسة في جميع النماذج: الأول، والثاني (التحليل الأساسي)، والثاني (تحليل الحساسية)، أكبر من (0.05)، وهذا يعني أن جميع المتغيرات تتبع التوزيع الطبيعي.

5-6-1-2 اختبار التداخل الخطي *Multi-Collinearity*

للتحقق من مدى وجود مشكلة التداخل الخطي بين متغيرات الدراسة المفسرة (المستقلة، والرقابية)، باستخدام مقياس *Collinearity Diagnostics*، وذلك من خلال حساب معامل التباين المسموح به *Tolerance* لكل متغير من تلك المتغيرات المفسرة، ومن ثم إيجاد معامل تضخم التباين *Variance Inflation factor (VIF)*، وهذا الاختبار يعد مقياساً لتأثير التداخل الخطي (أي الارتباط) بين المتغيرات المستقلة والرقابية. ويرى الإحصائيون المختصون مثل (Kutner et al., 2005)، أنه كلما كانت قيمة معامل *Tolerance* أكبر من (0.1)، وقيمة (*VIF*) أقل من (10)، فإن ذلك يعد كافياً للحكم على أن

المتغيرات المفسرة لا تعاني من وجود مشكلة التداخل الخطي المتعدد. والجدول رقم (5) يعرض نتائج هذا الاختبار:

جدول 5: نتائج اختبار التداخل الخطي المتعدد بين المتغيرات المفسرة باستخدام مقياس

Collinearity Diagnostics

Collinearity Diagnostics						المتغيرات المفسرة
النموذج الثاني (تحليل الحساسية)		النموذج الثاني (التحليل الأساسي)		النموذج الأول		
VIF	Tolerance	VIF	Tolerance	VIF	Tolerance	
1.098	0.911	1.038	0.964			CRD
				1.014	0.985	BSIZE
				1.091	0.917	BIND
				1.003	0.996	BDIV
1.087	0.934	1.087	0.934			SIZE
1.020	0.977	1.020	0.977			PROF
1.107	0.901	1.107	0.901			LEV
1.095	0.915	1.098	0.911			AUDIT

- المصدر: (الجدول من إعداد الباحثان من واقع نتائج التحليل الإحصائي).

بفحص قيم معامل Tolerance الواردة في جدول رقم (5) لجميع المتغيرات المفسرة (المستقلة والرقابية) والمتعلقة بجميع النماذج، تبين للباحثان أنها أكبر من (0.1)، كما أن جميع قيم معامل تضخم التباين (VIF) أقل من القيمة (10)، مما يدل على أن الارتباط بين جميع المتغيرات المفسرة ضعيف جداً، وعلى ذلك يمكن التأكيد على أن النماذج التطبيقية الخطية للدراسة لا تعاني من تعدد العلاقات الخطية، أو مشكلة التداخل (الازدواج) الخطي المتعدد.

5-6-1-3 اختبار علاقات الارتباط الأحادية بين متغيرات الدراسة

قام الباحثان باستخدام مصفوفة الارتباط الخطي البسيط لبيرسون *Pearson Correlation Matrix* من أجل اختبار علاقات الارتباط الأحادية *Univariate Correlation* بين متغيرات الدراسة. ويوضح الجدول رقم (6) نتائج اختبارات علاقات الارتباط الأحادية بين متغيرات الدراسة.

جدول 6: مصفوفة الارتباط الخطي البسيط لبيرسون لقياس علاقة الارتباط الأحادية بين متغيرات الدراسة

المتغيرات	المقياس	CRD	BFSIZE	BIND	BDIV	SP	SIZE	PROF	LEV	AUDIT
CRD	Corr.	1								
	Sig.									
BFSIZE	Corr.	0.506*	1							
	Sig.	0.000								
BIND	Corr.	0.409*	0.068	1						
	Sig.	0.032	0.524							
BDIV	Corr.	0.336*	0.251*	-0.111	1					
	Sig.	0.046	0.017	0.298						
SP	Corr.	-0.457*				1				
	Sig.	0.017								
SIZE	Corr.	0.112				0.587*	1			
	Sig.	0.296				0.000				
PROF	Corr.	-0.017				0.372*	0.053	1		
	Sig.	0.875				0.033	0.620			
LEV	Corr.	0.148				-0.554*	-0.144	-0.108	1	
	Sig.	0.165				0.011	0.187	0.149		
AUDIT	Corr.	-0.029				0.296*	0.129	0.146	-0.098	1
	Sig.	0.785				0.044	0.228	0.220	0.356	

*العلاقة ذات دلالة إحصائية عند مستوى معنوية (0.05) أو أقل.

يتضح من جدول رقم (6) ما يلي:

- توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين الإفصاح عن مخاطر الأمن السيبراني (CRD) وبين حجم مجلس الإدارة (BFSIZE)، حيث أن معامل الارتباط موجب ومستوى المعنوية (Sig) أقل من (0.01).

- ويتضح أيضا أنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين الإفصاح عن مخاطر الأمن السيبراني (CRD) وبين استقلال مجلس الإدارة (BINO)، حيث أن معامل الارتباط موجب ومستوى المعنوية (Sig) أكبر من (0.01).

- كما يتبين أنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين الإفصاح عن مخاطر الأمن السيبراني (CRD) وبين تنوع مجلس الإدارة (BDIV)، حيث أن معامل الارتباط موجب ومستوى المعنوية (Sig) أكبر من (0.01).

- ويلاحظ أنه توجد علاقة ارتباط سالبة ضعيفة وذات دلالة معنوية بين أسعار أسهم الشركة (SP) وبين الإفصاح عن مخاطر الأمن السيبراني (CRD)، حيث أن معامل الارتباط سالب ومستوى المعنوية (Sig) أكبر من (0.01).

- كما يلاحظ أنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين أسعار أسهم الشركة (*SP*) وبين حجم الشركة (*SIZE*)، حيث أن معامل الارتباط موجب ومستوى المعنوية (*Sig*) أقل من (0.01).
- كما يتضح أنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين أسعار أسهم الشركة (*SP*) وبين ربحية الشركة (*PROF*)، حيث أن معامل الارتباط موجب ومستوى المعنوية (*Sig*) أكبر من (0.01).
- كما يتبين أنه توجد علاقة ارتباط سالبة وذات دلالة معنوية بين أسعار أسهم الشركة (*SP*) وبين درجة الرفع المالي (*LEV*)، حيث أن معامل الارتباط سالبة ومستوى المعنوية (*Sig*) أكبر من (0.01).
- كما يتضح أنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين أسعار أسهم الشركة (*SP*) وبين حجم مكتب المراجعة (*AUDIT*)، حيث أن معامل الارتباط موجب ومستوى المعنوية (*Sig*) أكبر من (0.01).

بينما باقي علاقات الارتباط الأحادية سواء بين المتغيرات المستقلة، أو الرقابية، مع بعضها البعض، أو مع متغير أسعار الأسهم (*SP*)، كلها علاقات ارتباط غير معنوية.

وهكذا، يتضح من قيم وإشارات معاملات الارتباط الأحادية أنها تتسق مع ما توقعه الدراسة الحالية، حيث وجدت مؤشرات مبدئية على احتمال ظهور أثر لخصائص مجلس الإدارة علي الإفصاح عن مخاطر الأمن السيبراني وكذلك وجود أثر للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم، مما يمثل أساساً مناسباً لإمكانية اختبار فروض الدراسة الحالية من الناحية الإحصائية باستخدام نماذج الانحدار الخطي متعدد المتغيرات.

5-6-1-4 اختبار استقلال السلاسل الزمنية لمتغيرات الدراسة

للتحقق من استقرار السلاسل الزمنية *Time Series Stationary* لمتغيرات الدراسة، قام الباحثان باستخدام اختبارات جذور الوحدة *Unit Root Tests* لمعرفة مدى استقرار السلاسل الزمنية عبر الزمن، بحيث تكون السلسلة الزمنية مستقرة *Stationary* إذا كان هناك ثبات في قيمة الوسط الحسابي والتباين عبر الزمن. وقاعدة القرار في هذه الحالة هو قبول فرض الدراسة (وهو بأن السلسلة الزمنية مستقرة)، إذا كانت القيمة الاحتمالية *P-value* أقل من (0.05)، والعكس صحيح. ويوضح جدول رقم (7) نتائج اختبار استقرار السلاسل الزمنية لمتغيرات الدراسة.

جدول 7: نتائج اختبار استقلال السلاسل الزمنية لمتغيرات الدراسة

Unit Root Tests						المتغيرات المفصرة	
PP-Fisher (χ^2)		Augmented Dick-Fuller		Levin, Lin & Chu t values			
P-value	value	P-value	Value	P-value	Value		
0.000	237.52*	0.001	210.63*	0.000	-18.28*	BSIZE	المتغيرات المفصرة للنموذج الأول
0.002	89.34*	0.007	79.63*	0.002	-3.74*	BIND	
0.000	210.21*	0.002	220.17*	0.006	-12.15*	BDIV	
0.000	130.16*	0.000	141.69*	0.011	-6.08*	CRD	المتغيرات المفصرة والنوعية للنموذج الثاني (التحليل الأساسي)
0.000	178.58*	0.000	180.31*	0.015	-7.98*	SIZE	
0.000	189.57*	0.000	192.26*	0.017	-9.45*	PROF	
0.001	110.26*	0.008	71.82*	0.021	-3.64*	LEV	
0.000	251.52*	0.000	312.50*	0.000	-24.21*	AUDIT	
0.000	130.16*	0.000	141.69*	0.011	-6.08*	CRD	المتغيرات المفصرة والنوعية للنموذج الثاني (تحليل الحساسية)
0.000	178.58*	0.000	180.31*	0.015	-7.98*	SIZE	
0.000	189.57*	0.000	192.26*	0.017	-9.45*	PROF	
0.001	110.26*	0.008	71.82*	0.021	-3.64*	LEV	
0.000	267.18*	0.000	299.62*	0.000	-28.30*	AUDIT	

- المصدر: (الجدول من إعداد الباحثان من واقع نتائج التحليل الإحصائي).
 - * العلاقة ذات دلالة إحصائية عند مستوى معنوية (0.05) أو أقل.

يتضح من الجدول رقم (7)، أن القيمة الاحتمالية P -value لجميع متغيرات الدراسة أقل من (0.05)، وهو ما يشير إلى أن علاقات الانحدار بين متغيرات الدراسة، ليست علاقات انحدار زائفة *Spurious Regression*، أي أنها صالحة لتطبيق نماذج الانحدار الخطي متعدد المتغيرات عليها، ومن ثم رفض الفرض العدمي بأن السلاسل الزمنية لمتغيرات الدراسة ليست مستقرة.

5-6-2 الإحصاءات الوصفية لعينة الدراسة

في هذا البند سيتم عرض أهم الإحصاءات الوصفية لمتغيرات الدراسة التطبيقية.

ويوضح الجدول رقم (8) المتوسط الحساب والانحراف المعياري وأعلى وأدنى قيمة لمتغيرات الدراسة عن فترة الدراسة مجتمعة. وتشير الإحصاءات الوصفية الواردة بجدول (8) أن المتوسط الحسابي لمتغير الإفصاح عن مخاطر الأمن السيبراني عن فترة الدراسة مجتمعة بلغ (0.4899)، يضاف إلى ذلك أن هناك فرقاً كبيراً بين أعلى قيمة وأدنى قيمة، حيث بلغت أعلى قيمة وأدنى قيمة (0.70)، (0.05) على التوالي، لذلك فقد بلغ الانحراف المعياري لمتغير الإفصاح عن مخاطر الأمن السيبراني (0.08285).

وبالنسبة لحجم مجلس إدارة الشركة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (9.9778)، وأن الانحراف المعياري لهذا المتغير بلغ (3.02045)، وأن أعلى قيمة وأدنى قيمة بلغت (19.00)، (4.00) على التوالي. أما بالنسبة لمتغير استقلال مجلس الإدارة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (0.3377)، وأن الانحراف المعياري له قد بلغ (0.65334)، وأن هناك فرق كبير بين أعلى قيمة وأدنى قيمة حيث بلغتا (6.00)، (0.00) على التوالي. أما بالنسبة لتنوع مجلس الإدارة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (0.2949)، وأن الانحراف المعياري له قد بلغ (0.05744)، وأن هناك فرقا واضحا بين أعلى قيمة وأدنى قيمة حيث بلغتا (0.42)، (0.14) على التوالي. أما بالنسبة لأسعار الأسهم، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (1.5090)، وأن الانحراف المعياري له قد بلغ (6.92861)، وأن قيمتي أعلى قيمة وأدنى بلغتا (58.00)، (0.20) على التوالي. أما متغير حجم الشركة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (9.2792)، وأن الانحراف المعياري له قد بلغ (1.23153)، وأن قيمتي أعلى قيمة وأدنى بلغتا (11.20)، (4.47) على التوالي. وبالنسبة لربحية الشركة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (0.1117)، وأن الانحراف المعياري له قد بلغ (0.15677)، وأن قيمتي أعلى قيمة وأدنى بلغتا (0.84)، (0.00) على التوالي. وبالنسبة لدرجة الرفع المالي، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (0.5317)، وأن الانحراف المعياري له قد بلغ (0.25851)، وأن قيمتي أعلى قيمة وأدنى بلغتا (0.96)، (0.06) على التوالي. وبالنسبة لحجم مكتب المراجعة، فتشير الإحصاءات الوصفية إلى أن المتوسط الحسابي لهذا المتغير بلغ (0.6444)، وأن الانحراف المعياري له قد بلغ (0.48136)، وأن قيمتي أعلى قيمة وأدنى بلغتا (1.00)، (0.00) على التوالي. وهذه النتائج المتباينة تعتبر طبيعية في ظل عينة من صناعات مختلفة.

جدول 8: بعض الإحصاءات الوصفية لمتغيرات الدراسة عن فترة الدراسة مجتمعة (ن=90) *

الحد الأعلى	الحد الأدنى	الانحراف المعياري	المتوسط الحسابي	الإحصاءات الوصفية المتغير
0.70	0.05	0.08285	0.4899	الإفصاح عن مخاطر الأمن السيبراني
19.00	4.00	3.02045	9.9778	حجم مجلس الإدارة
6.00	0.00	0.65334	0.3377	استقلال مجلس الإدارة
0.42	0.14	0.05744	0.2949	تنوع مجلس الإدارة
58.00	0.20	6.92861	1.5090	أسعار الأسهم
11.20	4.47	1.23153	9.2792	حجم الشركة

0.84	0.00	0.15677	0.1117	ربحية الشركة
0.96	0.06	0.25851	0.5317	درجة الرفع المالي
1.00	0.00	0.48136	0.6444	حجم مكتب المراجعة

* عدد المشاهدات لفترة الدراسة مجتمعة (ن = 90 مشاهدة).

5-7 نتائج اختبار فروض البحث

تم استخدام أسلوب الانحدار المتعدد لاختبار فروض البحث السابق عرضها، حيث استخدم الباحثان نماذج الانحدار السابق عرضها. ويعرض الجدول رقم (9) ملخص نتائج التحليل الإحصائي لاختبار فروض البحث:

جدول 9: نتائج التحليل الإحصائي لنموذجي الانحدار

النموذج	المتغير التابع	المتغيرات التفسيرية	معاملات الانحدار (β)	قيمة اختبار (t)	مستوى الدلالة الفعلية P -value	قيمة اختبار (F) للنموذج	مستوى الدلالة الفعلية للنموذج	$Adjusted (R^2)$
الأول**	CRD	Constant	0.352	7.604*	0.000	10.013*	0.000	0.233
		BFSIZE	0.214	5.463*	0.000			
		BIND	0.186	3.523*	0.002			
		BDIV	0.117	2.120*	0.005			
الثاني***	SP (التحليل الأساسي)	Constant	-2.860	-0.649	0.518	7.412	0.008	0.314
		CRD	-0.918	-2.306	0.017			
		SIZE	0.282	0.386*	0.016			
		PROF	3.766	0.405*	0.046			
		LEV	-3.789	-0.783*	0.026			
		AUDIT	0.381	0.148*	0.038			
		Constant	-0.535	-0.047	0.963			
	SP (تحليل حساسية)	CRD	-0.357	-2.231	0.018			

* العلاقة ذات دلالة إحصائية عند مستوى معنوية (0.05) أو أقل.

** تم الاقتصار على عرض المتغيرات الخاصة بالنموذج الأول والتي تعتبر محل اهتمام الباحثان لاختبار الفروض: الأول والثاني والثالث.

*** تم الاقتصار على عرض المتغيرات الخاصة بالنموذج الثاني والتي تعتبر محل اهتمام الباحثان لاختبار الفروض الرابع.

5-7-1 نتائج اختبارات الفروض المتعلقة بنموذج الانحدار الأول: أثر خصائص مجلس الإدارة

على الإفصاح عن مخاطر الأمن السيبراني.

توضح نتائج التحليل الإحصائي بالجدول رقم (9) لنموذج الانحدار الأول أن معامل التحديد ($Adjusted R^2$) بلغ (0.233)، أي أن المتغيرات المستقلة (حجم مجلس الإدارة، استقلال مجلس الإدارة، تنوع مجلس الإدارة)، يفسرون حوالي (23.3%) من التغير الكلي في قيمة المتغير التابع (الإفصاح عن

مخاطر الأمن السيبراني). وفيما يتعلق بمدى معنوية نموذج الانحدار، فقد بلغت قيمة (F) المحسوبة للنموذج (10.013) وهي قيمة معنوية حيث بلغ مستوى الدلالة الفعلية للنموذج (0.000) وهي قيمة أقل من مستوى المعنوية المفترض (0.05). وهذا يشير إلى أن النموذج ككل يتمتع بمعنوية إحصائية عالية.

5-7-1-1 نتيجة اختبار الفرض الأول

استهدف الفرض الأول وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين حجم مجلس الإدارة ومستوى الإفصاح عن مخاطر الأمن السيبراني. وتوضح نتائج التحليل بجدول رقم (9) أن معامل الانحدار لمتغير حجم مجلس الإدارة قد بلغ (0.214)، وقيمة اختبار (t) بلغت (5.463)، وقيمة *P-value* بلغت (0.000)، ويشير ذلك إلى وجود تأثير إيجابي ومعنوي لحجم مجلس الإدارة على مستوى الإفصاح عن مخاطر الأمن السيبراني. وبالتالي يتم قبول الفرض الأول للبحث بأنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين حجم مجلس الإدارة ومستوى الإفصاح عن مخاطر الأمن السيبراني.

وهذا يتفق مع ما توصلت إليه دراسة (Saggar & Singh, 2017; Alkurdi et al., 2019) إلى أن حجم مجلس الإدارة الكبير له تأثير إيجابي علي إفصاح الشركة عن المخاطر، ودراسة (Hsu & Wang, 2014) التي توصلت إلى أن المجالس الأكبر حجماً والمجالس ذات المديرين الأكبر سناً والمدة الأطول ترتبط باحتمالية أقل للانتهاكات الأمنية، ويرجع ذلك إلى أن كبر حجم مجلس الإدارة يعزز من فعالية الدور الرقابي لمجلس الإدارة نظراً لتنوع الخبرة والمعرفة بين أعضائه، بما يسمح بتخصيص الواجبات بشكل أفضل وتقسيم المجلس إلى لجان متخصصة لمراقبة ومتابعة أعمال إدارة الشركة، ومن ثم سوف تساعد علي الإفصاح عن المزيد من المعلومات المتعلقة بمخاطر الأمن السيبراني، وإن كان ذلك يختلف مع دراسة (Smaili et al., 2022) التي توصلت إلى عدم وجود تأثير لحجم مجلس الإدارة علي مستوى الإفصاح عن مخاطر الأمن السيبراني.

5-7-1-2 نتيجة اختبار الفرض الثاني

استهدف الفرض الثاني وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين استقلال مجلس الإدارة ومستوى الإفصاح عن مخاطر الأمن السيبراني. وتوضح نتائج التحليل بجدول رقم (9) أن معامل الانحدار لمتغير استقلال مجلس الإدارة قد بلغ (0.186)، وقيمة اختبار (t) بلغت (3.523)، وقيمة *P-value* بلغت (0.002)، ويشير ذلك إلى وجود تأثير إيجابي ومعنوي لاستقلال مجلس الإدارة على مستوى الإفصاح عن مخاطر الأمن السيبراني. وبالتالي يتم قبول الفرض الثاني للبحث بأنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين استقلال مجلس الإدارة ومستوى الإفصاح عن مخاطر الأمن السيبراني.

وهذا يتفق مع ما توصلت إليه دراسة (Heroux & Fortin, 2021; Smaili et al., 2022) من وجود علاقة إيجابية ومعنوية بين استقلال مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، ويفسر الباحثان ذلك إلي أن المديرين المستقلون هم أشخاص محترفون ليس لديهم دور إداري أو علاقة مع الشركة من خلال العمل أو الملكية ولديهم سمعة النزاهة المهنية، بالإضافة إلي أن وجود أعضاء مستقلون داخل مجلس الإدارة يساعد علي زيادة الدور الرقابي علي المديرين التنفيذيين ويحد من تعارض المصالح بين الإدارة والملاك، وبالتالي قد يكون المديرين المستقلون أكثر ميلاً لتشجيع الشركات علي القيام بالمزيد من الإفصاح عن المعلومات المتعلقة بمخاطر الأمن السيبراني، وإن كان ذلك يختلف عن دراسة (Hsu & Wang, 2014) التي توصلت إلي أن المجالس التي بها نسبة مئوية أكبر من المستقلين ترتبط بشكل إيجابي مع احتمالية حدوث انتهاكات أمنية، ويرجع ذلك إلي أن المديرين الخارجيين قد لا يكون لديهم معرفة داخلية كافية بالشركة للمساهمة في تقليل احتمالية حدوث انتهاكات أمنية.

5-7-1-3 نتيجة اختبار الفرض الثالث

استهدف الفرض الثالث وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني. وتوضح نتائج التحليل بجدول رقم (9) أن معامل الانحدار لمتغير تنوع مجلس الإدارة قد بلغ (0.117)، وقيمة اختبار (t) بلغت (2.120)، وقيمة P -value بلغت (0.005)، ويشير ذلك إلي وجود تأثير إيجابي ومعنوي لتنوع مجلس الإدارة على مستوي الإفصاح عن مخاطر الأمن السيبراني. وبالتالي يتم قبول الفرض الثالث للبحث بأنه توجد علاقة ارتباط إيجابية وذات دلالة معنوية بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني.

وهذا يتفق مع ما توصلت إليه دراسة (Heroux & Fortin, 2021; Radu, & Smaili, 2022; Remeis, 2023) من وجود علاقة إيجابية ومعنوية بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، ويفسر الباحثان ذلك إلي أن وجود الإناث بمجلس الإدارة قد يساعد علي زيادة فعالية المجلس وتحسين وظيفة وكفاءة اللجان المنبثقة منه، بما يعكس علي تحسين جودة الإشراف علي القرارات الإدارية المتعلقة بمسائل الأمن السيبراني من خلال تنوع مستوي الخبرة، وأنماط الاتصال والإدراك، بالإضافة إلي أن الإناث لديهن معايير أخلاقية أعلى وأكثر نفوراً من المخاطر، وأكثر التزاماً بحضور الاجتماعات بمعدلات أعلى من الذكور مما يؤدي إلي ارتفاع جودة المناقشات والتشاور وتقديم وجهات نظر مختلفة إلي مجلس الإدارة حول عوامل مخاطر الأمن السيبراني وأدوات التخفيف من مخاطر الأمن السيبراني، وهذا يؤدي إلي مزيد من الشفافية والإفصاح عن هذه المعلومات.

ومما سبق يمكن صياغة نموذج الانحدار لأثر خصائص مجلس الإدارة على الإفصاح عن مخاطر الأمن السيبراني كما يلي.

$$CRD = 0.352 + 0.214(BSIZE) + 0.186(BIND) + 0.117(BDIV)$$

5-7-2 نتائج اختبارات الفروض المتعلقة بنموذج الانحدار الثاني: أثر الإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم

فيما يخص نموذج الانحدار الثاني والذي استهدف دراسة أثر الإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم، فإن نتائج التحليل الإحصائي بالجدول رقم (9) توضح أن معامل التحديد (*Adjusted R2*) قد بلغ (0.314)، أي أن المتغير المستقل (الإفصاح عن مخاطر الأمن السيبراني) والمغيرات الرقابية (حجم الشركة، وربحية الشركة، ودرجة الرفع المالي، وحجم مكتب المراجعة)، يفسرون ما نسبته حوالي (31.4%) من التغير الكلي في قيمة المتغير التابع (أسعار الأسهم). وفيما يتعلق بمدى معنوية نموذج الانحدار، فقد بلغت قيمة (*F*) المحسوبة للنموذج (7.412) وهي قيمة معنوية حيث بلغ مستوى الدلالة الفعلية للنموذج (0.008) وهي قيمة أقل من مستوى المعنوية المفترض (0.05).

5-7-2-1 نتيجة اختبار الفرض الرابع

استهدف الفرض الرابع وجود أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم.

وتوضح نتائج التحليل بجدول رقم (9) النموذج الثاني (التحليل الأساسي)، أن معامل الانحدار لمتغير الإفصاح عن مخاطر الأمن السيبراني قد بلغ (-0.918)، وقيمة اختبار (*t*) بلغت (-2,306)، وقيمة *P-value* بلغت (0.017)، ويشير ذلك إلى وجود تأثير سلبي ومعنوي للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم. وبالتالي يتم قبول الفرض الرابع للبحث بأنه يوجد أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم.

وهذا يتفق مع ما توصلت إليه دراسة كل من (Goel & Shawky, 2014; kamiya et al., 2021)، الرشيد، السيد، 2019؛ إلي وجود علاقة سلبية بين الإفصاح عن مخاطر الأمن السيبراني وأسعار الأسهم، ويرجع ذلك إلي أن المستثمرين يتأثرون بالمعلومات المفصح عنها حول الهجمات والاختراقات السيبرانية والتي تقلل من رغبتهم في الاستثمار، مما يؤثر سلباً علي سمعة الشركة وأسعار أسهمها، وإن كان ذلك يختلف عن دراسة (Gordon et al., 2010; Spanos & Angelis, 2016).

(Masuch et al., 2022; Szubartowicz & Schryen, 2020) التي توصلت إلي وجود علاقة إيجابية معنوية بين الإفصاح عن معلومات الأمن السيبراني وأسعار الأسهم.

5-7-2-2 تحليل الحساسية (إعادة اختبار الفرض الرابع)

تم إجراء تحليل الحساسية بإعادة اختبار الفرض الرابع والذي استهدف وجود أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم، حيث تم قياس سعر السهم باستخدام التغير في سعر السهم، وهو عبارة عن الفرق بين سعر الإغلاق في سنة القياس والسنة السابقة لها، من خلال المقياس التالي:

سعر الإغلاق في سنة القياس - سعر الإغلاق في السنة السابقة / سعر الإغلاق في السنة السابقة، وذلك قياساً على (Jizi & Dixon, 2016؛ الصيرفي، 2018).

وذلك بعد أن تم قياس سعر السهم في التحليل الأساسي بسعر الإقبال للسهم في اليوم التالي لتاريخ تقرير مراقب الحسابات، أو أول جلسة تداول بعد تاريخ تقرير مراقب الحسابات، وذلك قياساً على (Ge et al., 2021; Vazakidis et al., 2013; Nasution & Mita, 2017)

وتوضح نتائج التحليل بجدول رقم (9) النموذج الثاني (تحليل الحساسية)، أن معامل الانحدار لمتغير الإفصاح عن مخاطر الأمن السيبراني قد بلغ (-0.357)، وقيمة اختبار (t) بلغت (-2.231)، وقيمة P -value بلغت (0.018)، ويشير ذلك إلى وجود تأثير سلبي ومعنوي للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم. وبالتالي يتم قبول الفرض الرابع للبحث بأنه يوجد أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم، وهذه نفس النتيجة التي تم التوصل إليها في التحليل الأساسي رغم اختلاف طريقة القياس.

5-7-2-3 النتائج المتعلقة بالمتغيرات الرقابية

وفيما يتعلق بالمتغيرات الرقابية في نموذج الانحدار الثاني، فتشير نتائج التحليل الإحصائي بالجدول رقم (9) إلى وجود علاقة موجبة ومعنوية بين متغير حجم الشركة، ومتغير ربحية الشركة، ومتغير حجم مكتب المراجعة، وبين أسعار الأسهم. بينما تشير النتائج أيضاً إلى وجود علاقة سالبة ومعنوية بين متغير درجة الرفع المالي وبين أسعار الأسهم. ويرجع ذلك إلى أن الشركات ذات الحجم الكبير لديها حوافز كبيرة للحد من مخاوف المستثمرين من خلال زيادة مستوى الإفصاح للحد من مشكلة عدم تماثل المعلومات وبالتالي جذب المزيد من المستثمرين مما ينعكس إيجابياً على أسعار الأسهم، وكلما زادت ربحية الشركة كلما دل ذلك على حسن استغلال إدارة الشركة لأصولها في توليد الأرباح، مما يؤدي إلى ارتفاع أسعار أسهم الشركة، وكلما زاد حجم مكتب المراجعة وتمت المراجعة بواسطة شركات المراجعة الأربعة الكبرى

كلما ارتفعت جودة التقرير المالي، الأمر الذي يؤدي إلى تخفيض المخاطر في سوق الأوراق المالية وتخفيض الأخطاء والمخالفات، مما ينعكس إيجابياً علي أسعار الأسهم، وكلما ارتفعت درجة الرفع المالي كلما زاد من تعرض الشركة للمخاطر، مما ينعكس سلباً علي أسعار الأسهم .

ومما سبق يمكن صياغة نموذج الانحدار لأثر الإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم كما يلي:

$$SP = -2.860 - 0.918 (CRD) + 0.282 (SIZE) + 3.766 (PROF) - 3.789 (LEV) + 0.381 (AUDIT)$$

6- النتائج والتوصيات ومجالات البحث المستقبلية

6-1 النتائج

في إطار هدف ومنهج البحث تتمثل أهم نتائج البحث فيما يلي:

- يُعد مجلس الإدارة من أهم آليات حوكمة الشركات، ويمثل السلطة العليا التي تحكم وتدير الشركة بناءً علي تفويض من الجمعية العامة للمساهمين، فهو مسئول عن صياغة استراتيجية الشركة ومتابعة تنفيذها، بصورة تساعد علي تحقيق أهداف الشركة وتوفير الحماية اللازمة لأصحاب المصالح والحد من تضارب هذه المصالح، ومع زيادة الهجمات السيبرانية التي تتعرض لها الشركات أصبح الأمن السيبراني والمخاطر السيبرانية من أهم القضايا المطروحة علي مجلس الإدارة، وأصبحت مجالس الإدارة مسؤولة عن الإشراف على قيام الشركة بإنشاء برامج مناسبة لإدارة المخاطر والإشراف على كيفية تنفيذ الإدارة لتلك البرامج وتقديم المشورة للإدارة عند اتخاذ القرارات المتعلقة بالأمن السيبراني لحماية أصحاب المصالح.

- أن الإفصاح عن مخاطر الأمن السيبراني يساهم في تخفيض عدم تماثل المعلومات ويساعد أصحاب المصالح علي تقييم مدي قدرة الشركة علي الحفاظ علي أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، كما يُعد إحدى الطرق لزيادة المصداقية وحماية ومساعدة المستثمرين علي اتخاذ قراراتهم الاستثمارية مما ينعكس علي أسعار الأسهم، كما يقلل من تكاليف النقاضي المحتملة التي قد تتعرض لها الشركات، مما ينعكس علي الأداء المالي، وبالتالي يؤثر علي سُمعة الشركة وأسعار الأسهم والتدفق النقدي المستقبلي.

- وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين حجم مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، حيث كانت القيمة الاحتمالية (P.value) أقل من مستوى المعنوية (0.05)، وهو ما

يثبت صحة الفرض الأول، ويرجع ذلك إلى أن كبر حجم مجلس الإدارة يعزز من فعالية الدور الرقابي لمجلس الإدارة نظراً لتنوع الخبرة والمعرفة بين أعضائه، بما يسمح بتخصيص الواجبات بشكل أفضل وتقسيم المجلس إلى لجان متخصصة لمراقبة ومتابعة أعمال إدارة الشركة، ومن ثم سوف تساعد علي الإفصاح عن المزيد عن المعلومات المتعلقة بمخاطر الأمن السيبراني.

- وجود علاقة ارتباط إيجابية وذات دلالة معنوية بين استقلال مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، حيث كانت القيمة الاحتمالية (P.value) أقل من مستوى المعنوية (0.05)، وهو ما يثبت صحة الفرض الثاني، وهذا يتفق مع ما توصلت إليه دراسة (Heroux & Fortin, 2021; Smaili et al., 2022) ويفسر الباحثان ذلك إلى أن وجود أعضاء مستقلون داخل مجلس الإدارة يساعد علي زيادة الدور الرقابي علي المديرين التنفيذيين ويحد من تعارض المصالح بين الإدارة والملاك، وبالتالي قد يكون المديرين المستقلون أكثر ميلاً لتشجيع الشركات علي القيام بالمزيد من الإفصاح عن المعلومات المتعلقة بمخاطر الأمن السيبراني.

- هناك علاقة ارتباط إيجابية وذات دلالة معنوية بين تنوع مجلس الإدارة ومستوي الإفصاح عن مخاطر الأمن السيبراني، حيث كانت القيمة الاحتمالية (P.value) أقل من مستوى المعنوية (0.05)، وهو ما يثبت صحة الفرض الثالث، وهذا يتفق مع ما توصلت إليه دراسة (Heroux & Fortin, 2021; Radu, & Smaili, 2022; Remeis, 2023) ويفسر الباحثان ذلك إلى أن وجود الإناث بمجلس الإدارة قد يساعد علي زيادة فعالية المجلس وتحسين وظيفة وكفاءة اللجان المنبثقة منه، بما ينعكس علي تحسين جودة الاشراف علي القرارات الإدارية المتعلقة بمسائل الأمن السيبراني من خلال تنوع مستوي الخبرة، بالإضافة إلي أن الإناث لديهن معايير أخلاقية أعلى وأكثر نفوراً من المخاطر، وأكثر التزاماً بحضور الاجتماعات بمعدلات أعلى من الذكور مما يؤدي إلي ارتفاع جودة المناقشات والتشاور وتقديم وجهات نظر مختلفة إلي مجلس الإدارة حول عوامل مخاطر الأمن السيبراني وأدوات التخفيف من مخاطر الأمن السيبراني، وهذا يؤدي إلي مزيد من الشفافية والإفصاح عن هذه المعلومات.

- هناك أثر ذات دلالة معنوية للإفصاح عن مخاطر الأمن السيبراني على أسعار الأسهم (وهذا الأثر سلبي)، وهو ما يثبت صحة الفرض الرابع، وهذا يتفق مع ما توصلت إليه دراسة كل من (Goel & Shawayky, 2014; kamiya et al., 2021)؛ الرشيدى، السيد، 2019 ويرجع ذلك إلي أن المستثمرين يتأثرون بالمعلومات المفصح عنها حول الهجمات والاختراقات السيبرانية والتي تقلل من رغبتهم في الاستثمار، مما يؤثر سلباً علي سمعة الشركة وأسعار أسهمها.

- وجود علاقة موجبة ومعنوية بين كل من حجم الشركة، ربحية الشركة، وحجم مكتب المراجعة، وبين أسعار الأسهم، بينما توجد علاقة سالبة ومعنوية بين درجة الرفع المالي وبين أسعار الأسهم.

6-2 التوصيات

في ضوء النتائج التي تم التوصل إليها فإنه يمكن التوصية بما يلي:

- قيام الهيئات والمنظمات المهنية المسئولة عن إصدار معايير المحاسبة المصرية بإصدار معيار محاسبي ينظم المحاسبة عن مخاطر الأمن السيبراني، مع الأخذ في الاعتبار تجارب الدول الأخرى التي ألزمت شركاتها بالإفصاح عن مخاطر الأمن السيبراني، بما يساهم في تحسين جودة الإفصاح، وكذلك إصدار معيار مراجعة لبيان مسئولية مراقب الحسابات تجاه هذه المخاطر، بما يساعد جميع أصحاب المصالح على تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل.
- الإستعانة بالمؤشر المقترح في الدراسة لقياس مستوى الإفصاح عن مخاطر الأمن السيبراني، حيث يتسم بالشمول لمعظم أنواع مخاطر الأمن السيبراني وآثارها السلبية، وحوكمة إدارة مخاطر الأمن السيبراني وحماية الأمن السيبراني، وهو ما قد يوفر معلومات مفيدة لأصحاب المصالح تساعد على تقييم الأداء المستقبلي للشركة.
- توجيه اهتمام الشركات المسجلة بالبورصة إلي زيادة الإفصاح عن مخاطر الأمن السيبراني، لإعلام المستثمرين بكافة مخاطر الأمن السيبراني المحتملة والفعلية، التي قد تؤثر علي أدائها المالي، والإفصاح عن إجراءات وإدارة هذه المخاطر والحد منها، بما يساعد المستثمرين علي ترشيد قراراتهم الاستثمارية. كما يجب علي الشركات عقد ورش عمل ودورات تدريبية للموظفين حول الأمن السيبراني.
- توجيه اهتمام هيئة الرقابة المالية إلي تقييم الشركات المسجلة بالبورصة حسب جودة إفصاحها عن مخاطر الأمن السيبراني، مع فرض عقوبات صارمة علي الشركات التي لم تلتزم بالإفصاح عن تعرضها لحوادث سيبرانية، وهو ما يعزز من ثقة أصحاب المصالح في التقارير المالية المنشورة.
- ضرورة تركيز مناهج التعليم المحاسبي في الجامعات المصرية بالشكل الذي يساعد على تدريس الموضوعات المختلفة والمتعلقة بمخاطر الأمن السيبراني وإدارتها، للمساهمة في إعداد خريجين قادرين على التعامل مع مثل هذه المخاطر والحد منها.

3-6 مجالات البحث المستقبلية

يري الباحثان في ضوء ما تم التوصل إليه من نتائج وجود العديد من المجالات التي يمكن أن تشكل أساساً لبحوث مستقبلية من أهمها:

- تناولت الدراسة بعض خصائص مجلس الإدارة كمحددات للإفصاح عن مخاطر الأمن السيبراني، وهو ما يفتح المجال نحو مزيد من الدراسات في هذا الصدد تتناول خصائص أخرى من آليات الحوكمة بخلاف ما تناولته الدراسة الحالية مثل: عدد اجتماعات مجلس الإدارة، ازدواجية مناصب رئيس مجلس الإدارة والمدير التنفيذي، هيكل الملكية، لجنة المراجعة، الرقابة الداخلية، المراجعة الخارجية.
- العلاقة بين درجة حوكمة الشركات والإفصاح عن مخاطر الأمن السيبراني وأثره علي أسعار الأسهم.
- محددات الإفصاح عن مخاطر الأمن السيبراني وأثره علي خطر انهيار أسعار الأسهم، دراسة تطبيقية علي الشركات المسجلة في البورصة المصرية.
- تحليل العلاقة بين خصائص الشركة والإفصاح عن مخاطر الأمن السيبراني وأثرها على الأداء المالي: دراسة تطبيقية على الشركات المسجلة في البورصة المصرية.
- قياس أثر جودة الإفصاح عن مخاطر الأمن السيبراني على القدرة التنبؤية للمعلومات المحاسبية وأسعار الأسهم للشركات المسجلة في البورصة المصرية.
- أثر الإفصاح عن مخاطر الأمن السيبراني علي كفاءة الاستثمار، دراسة تطبيقية.

المراجع

أولاً: المراجع باللغة العربية

- الإستراتيجية الوطنية للأمن السيبراني، (2017-2021)، المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء جمهورية مصر العربية، ص ص 1-19.
- أمين، أسامة ربيع، (2013)، "التحليل الإحصائي للمتغيرات المتعددة باستخدام برنامج SPSS"، كلية التجارة، جامعة المنوفية، بدون ناشر، ص ص 135-150.
- الجوهري، إبراهيم السيد محمد، سليمان، حامد نبيل حامد، (2021)، " أثر هيكل الملكية علي العلاقة بين تنوع مجلس الإدارة وجودة الأرباح بالتطبيق علي الشركات المدرجة بالبورصة المصرية"، *المجلة العلمية للبحوث والدراسات التجارية*، كلية التجارة وإدارة الأعمال، جامعة حلوان، المجلد 45، العدد 4، ص ص 195 - 263.
- الدليل التنظيمي للأمن السيبراني، (2020)، هيئة الاتصالات وتقنية المعلومات، السعودية، ص ص 1-54. متاح علي www.fra.gov.eg.
- الدليل المصري لحوكمة الشركات (2016)، مركز المديرين المصري، الهيئة العامة للرقابة المالية، جمهورية مصر العربية، الإصدار الثالث.
- شرف، إبراهيم أحمد إبراهيم، (2023)، " أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين - دراسة تجريبية"، *مجلة الإسكندرية للبحوث المحاسبية*، كلية التجارة، جامعة الإسكندرية، المجلد 7، العدد 1، ص ص 211-282.
- الصيرفي، أسماء أحمد أحمد، (2018)، "أثر مستوي إفصاح البنوك التجارية عن ممارسات إدارة المخاطر علي أسعار الأسهم، دراسة تطبيقية علي البنوك التجارية المقيدة بالبورصة المصرية"، *مجلة الإسكندرية للبحوث المحاسبية*، كلية التجارة، جامعة الإسكندرية، المجلد 2، العدد 2، ص ص 133 - 199.
- على، محمود أحمد أحمد، و علي، صالح علي صالح، (2022)، "أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية"، *مجلة الإسكندرية للبحوث المحاسبية*، كلية التجارة، جامعة الإسكندرية، المجلد 6، العدد 3، ص ص 1-48

علي، إبراهيم زكريا عرفات، عتش، عبده أحمد عبده، (2012)، " أثر مشاركة المرأة في مجلس الإدارة علي فعالية في تحقيق أهداف حوكمة الشركات: دراسة تطبيقية في بيئة الأعمال المصرية"، مجلة الدراسات التجارية المعاصرة، كلية التجارة، جامعة كفر الشيخ، المجلد 7، العدد 11، الجزء الأول، ص ص 185 - 217.

مراد، دعاء يحيى مصطفى محمود، (2021)، " أثر مستوي الإفصاح عن المخاطر علي أسعار وحجم تداول أسهم الشركات في سوق الأوراق المالية المصرية - دراسة اختبارية"، رسالة ماجستير غير منشورة، كلية التجارة، جامعة الزقازيق ، ص ص 1-134.

موسي، بوسي حمدي، (2023)، " العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتاعب المراجعة الدور المعدل لسمات منشأة المحاسبة والمراجعة: دراسة تجريبية"، مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، المجلد 10، العدد 3، ص ص 387-458.

موسي، عمرو عادل عبدالفتاح، شاهين، عبدالحميد أحمد أحمد، شحاتة، محمد موسي علي، البحيري، مروة أحمد عبدالرحمن، (2023)، " قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية علي قيمة المنشأة، دراسة تطبيقية"، المجلة العلمية للدراسات والبحوث المالية والإدارية، كلية التجارة، جامعة مدينة السادات، المجلد 15، العدد3، ص ص 1 - 66.

هيئة السوق المالية السعودية، (2019)، الدليل الإسترشادي للأمن السيبراني لمؤسسات السوق المالية.

الهيئة العامة للرقابة المالية، قرار رقم (123،124) لسنة 2019 بشأن تعديل قواعد قيد وشطب الأوراق المالية بالبورصة المصرية.

الهيئة الوطنية للأمن السيبراني، (2018)، الضوابط الأساسية للأمن السيبراني، السعودية، ص ص 1-

40

يعقوب، إبتهاال إسماعيل، وهاب، اسعد محمد علي، الفرطوسي، علي سموم، (2022)، " مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية علي وفق المتطلبات الدولية: دراسة اختبارية"، مجلة الدراسات المالية والمحاسبية والإدارية، جامعة العربي بن مهدي أم البواقي، المجلد 9، العدد 1، ص ص 1403 - 1430.

ثانياً: المراجع باللغة الأجنبية

- Abdullah, M. D. F. (2019, November). "The Effect of Corporate Risk Disclosure toward Firm Value in Indonesia Sharia Stock Index", In IOP Conference Series: Materials Science and Engineering, 662 (3), 032070.
- Aguilar, L. A. (2014). "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus", Cyber Risks and the Boardroom Conference, New York Stock Exchange, (June 10). New York, NY: SEC. 1-17, Available at: <https://www.sec.gov/news/speech/2014-spch061014laa>
- Alkurdi, A., Hussainey, K., Tahat, Y., & Aladwan, M. (2019). "The impact of corporate governance on risk disclosure: Jordania evidence", **Academy of Accounting and Financial Studies Journal**, 23(1): 1-16, Available at: <https://www.abacademies.org/articles/the-impact-of-corporate-governance-on-risk-disclosure-jordanian-evidence-7886.html>.
- Al-Sartawi, A.M. (2020). "Information technology governance and cybersecurity at the board level", **International Journal of Critical Infrastructures**, 16(2):150-161.
- Al -Yahyaee, K. H., Al-Hadi, A. K., & Hussain, S. M. (2017). Market Risk Disclosures and Board Gender Diversity in Gulf Cooperation Council (GCC) Firms. *International Review of Finance*, 17(4), 645-658. Available at: <https://doi.org/10.1111/irfi.12123>
- Alzead, R., (2017). "The determinants and economic consequences of risk disclosure: Evidence from Saudi Arabia. PhD, Portsmouth Business School, University of Portsmouth, United Kingdom.
- Al-Zyoud, A, M. (2020). "Managing Cybersecurity Risks in Jordanian Banks", **Millennium Journal of Economic and Administrative Sciences**, 1 (1): 5-14, Available at: <https://doi.org/10.47340/mjeas.v1i1.2.2020>.

- 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. & Soderstorm, N. (2018). "Cybersecurity Awareness and Market Valuations", **Journal of Accounting and Public Policy**, 37(6): 508-526.
- Blonder, S.P. (2014). "How closely is the board paying attention to cyber risks?", Inside Counsel (formerly Corporate Legal Times), Available at: <http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber>.
- Bujno, M., C. Hitchcock, K. Parson, B. Lamm, D. DeHass, and H. Phillips. 2018. Risk oversight and the role of the board. Deloitte (October 2). Available at: <https://deloitte.wsj.com/riskandcompliance/2018/10/02/risk-oversightand-the-role-of-the-board/>
- CPA Canada. 2017. Cyber security risks and incidents: Reassessing your disclosure practices.
- Cheng, X., & Walton, S. (2019). "Do nonprofessional investors care about how and when data breaches are disclosed?", **Journal of Information Systems**, 33 (3), 163-182.
- Cossin, D., & Lu, A. (2021). "Board Oversight of Cyber Risks and Cybersecurity", Imd Global Board Center, Available at: <https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/>
- CSA (Canadian Securities Administrator), 2017, Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents.

Dakin, R. (2012). SEC cyber risk disclosure guidance. Available at:

<https://www.omegasecure.com/wp-content/uploads/2016/03/>

[Coalfire-Perspective-SEC-Cyber-Risk-Disclosure-Guidance.](#)

Du, C., Song, L. and Wu, J., (2016). "Bank accounting disclosure, information content in stock prices, and stock crash risk: Global evidence". *Pacific Accounting Review*, 28(3), 260-278.

Elamer, A. A., Ntim, C. G., Abdou, H. A., & Pyke, C. (2019), "Sharia supervisory boards, governance structures and operational risk disclosures: Evidence from Islamic banks in MENA countries", **Global Finance Journal**, 23(4): 331-356.

EY. (2020). What companies are disclosing about cybersecurity risk and oversight in 2020. EY Center for Board Matters, Available at: <https://ey.com/us/boardmatters>.

Florakis, C., C. Louca, R. Michaely, & M. Weber. (2020). "Cybersecurity Risk" 1-73, Available at: <http://ssrn.com>.

Gao, L., Calderon, T., & Calderon, F. (2020). "Public companies' cybersecurity risk disclosures", **International Journal of Accounting Information Systems**, 38(1):100468.

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

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

Hartmann, C. C., & Carmenate, J. (2021). "Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research". **American Accounting Association** 15(2): 9-23.

- Héroux, S., & Fortin, A. (2021). "Board of directors' impact on cybersecurity disclosure", ESG-UQAM, Cahier de recherche, 4:1-28, Available at: <http://www.cifo.uqam.ca/publications>.
- Higgs, J. L., Pinsker, R. E., Smith, T., & Young, G. R. (2016). "The relationship between board-level technology committees and reported security breaches", **Journal of Information Systems**, 30 (3): 79-98. <https://doi.org/10.2308/isys-51402>.
- Hilary, G., Segal, B., and Zhang, M. H. (2016). "Cyber-risk disclosure: who cares?", Georgetown McDonough School of Business Research Paper, (2852519), Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852519
- Hsu, C., and Wang, T. (2014). "Exploring the association between board structure and information security breaches", **Asia Pacific Journal of Information Systems**, 24 (4): 531-557, Available at: <https://dx.doi.org/10.14329/apjis.2014.24.4.531>
- Hussainey, K., & Al-Najjar, B. (2012). "Understanding the Determinants of Risk Metrics/ISS Ratings of the Quality of UK Companies' Corporate Governance Practice", **Canadian Journal of Administrative Sciences**, 29(4), 366-377. Available at: <https://doi.org/10.1002/cjas.1227>
- Idan, H. Z., Rapani, N. H. A., Khalid, A. A., & Al-Waeli, A. J. (2021). "The Effect of Corporate Governance Attributes on Corporate Social Responsibility Disclosure in Iraqi Companies: A Literature Review", **Journal of Contemporary Issues in Business and Government**, 27(2), 2778-2816.
- Information Systems Audit and Control Association (ISACA). (2017). Available at: <https://csrc.nist.gov/glossary/term/cybersecurity>

- Islam, M.S., Farah, N. and Stafford, T.F. (2018), "Factors associated with security/cybersecurity audit by internal audit function: An international study", **Managerial Auditing Journal**, 33 (4) : 377-409, Available at: <https://doi.org/10.1108/MAJ-07-2017-1595>.
- Juma'h, A. H., & Alnsour, Y. (2021). How Do Investors Perceive the Materiality of Data Security Incidents. **Journal of Global Information Management**, 29(6), 1-32.
- Kahyaoglu, S. B., & Caliyurt, K. (2018). "Cyber security assurance process from the internal audit perspective", **Managerial Auditing Journal**, 33 (4), 360-376.
- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", **Journal of Financial Economics**, 139 (3), 719-749.
- Kelton, A. S., & Pennington, R. R. (2020). "Do voluntary disclosures mitigate the cybersecurity breach contagion effect?", **Journal of Information Systems**, 34 (3): 133-157 Available at: <https://doi.org/10.2308/isys-52628>.
- Khalil, A., & Maghraby, M. (2017) "The determinants of internet risk disclosure: empirical study of Egyptian listed companies", **Managerial Auditing Journal**, 32(8):746-767.
- Kouaib, A., & Almulhim, A. (2019). "Earnings manipulations and board's diversity: The moderating role of audit", **The Journal of High Technology Management Research**, 30 (2), 100356.
- Kutner, Micheal H. et al. (2005). "**Applied Linear Statistical Models**", 5th Edition, McGraw Hil/Irwin, New York.
- Lankton,N., B. Price,J.,& Karim,M.(2021)." Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters", **Journal of Information Systems**, 35 (1): 101-119.

- Li, H., No, W. and Wang, T. (2018). "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors", **International Journal of Accounting Information Systems**, 30 (c): 40-55.
- Lim, R. (2011). "Are corporate governance attributes associated with accounting conservatism?", **Accounting and Finance** ,51 (4): 1007-1030.
- Martinez-Jimenez, R., Hernández-Ortiz,M,J., Fernández, C., & Ana , I. (2020). "Gender diversity influence on board effectiveness and business performance". **Corporate Governance: The International Journal of Business in Society**, 20(2):307-323 .
- Masuch, K., Greve, M., Trang, S., & Kolbe, L. M. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies?. *Computers & Security*, 112, 102502.
- Mattucci, J. (2023). " The Market's Reaction to the Disclosure of a Cybersecurity Breach", Honors Theses and Capstones. 766. <https://scholars.unh.edu/honors/766>
- Moumen,N., Othman,H,B., & Hussainey, K. (2016)."Board structure and the informativeness of risk disclosure: Evidence from MENA emerging markets", *Advances in Accounting, Incorporating Advances in International Accounting*, 35: 82-97.
- Mustafa, A. S., Che-Ahmad, A., and Chandren, S. (2017). "Board diversity and audit quality: Evidence from Turkey". **Journal of Advanced Research in Business and Management Studies**, 6 (1), 50-60.
- National institute of standards and technology (NIST) .(2018). a Glossary of key information security terms National institute of standards and technology interagency or internal report, Available at: <http://csrc.nist.gov/publications>.
- Newman, C. A. (2018). "When to Report a Cyberattack? For Companies, That's Still a Dilemma." *New York Times*, Gale Academic OneFile, Available at: gale.com/apps/doc/A529932029/AONE?

- Radu, C., & Smaili, N. (2022). "Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure", **Journal of Business Ethics**, 177(2):351-374.
- Remeis, K. (2023). "Board Gender Diversity and Cybersecurity Disclosure Characteristics", **Honors Theses and Capstones**. 742. Available at: <https://scholars.unh.edu/honors/742>.
- Saggar, R., and B., Singh. (2017). "Corporate Governance and Risk Reporting: Indian Evidence", **Managerial Auditing Journal**. 32(4/5): 1-39.
- SEC. (2011). CF disclosure guidance: Topic No. 2 cybersecurity. Washington, DC. Retrieved from: <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>
- SEC. (2018). Commission statement and guidance on public company cybersecurity disclosures. Washington DC Retrieved from: <https://www.sec.gov/rules/interp/2018/33-10459.pdf>
- SEC. (2022). Cybersecurity risk management for investment advisers, registered investment companies, and business development companies. Washington DC, Retrieved from: <https://www.sec.gov/rules/proposed/2022/33-11028.pdf>.
- Sharton, B. R. (2020). Will Coronavirus Lead to More Cyber Attacks?. <https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks?autocomplete=true> (accessed 20 October 2020).
- Shukla, M., & Pandey, P. (2023). "Cybersecurity Oversight and Board Diversity: The Disclosure Paradigm", *Cyberfeminism and Gender Violence in Social Media* (pp.151-173). DOI:[10.4018/978-1-6684-8893-5.ch010](https://doi.org/10.4018/978-1-6684-8893-5.ch010).
- Smaili, N. Radu, C., & Khalili, A. (2022). "Board effectiveness and cybersecurity disclosure", **Journal of Management and Governance**, Available at: [10.1007/s10997-022-0963](https://doi.org/10.1007/s10997-022-0963)

- Spanos, G. & Angeli, L.(2016). " The impact of information security events to the stock market: a systematic literature review", **Computers & Security**, 58: 216-229.
- Szubartowicz, E., & Schryen, G. (2020). "Timing in information security: An event study on the impact of information security investment announcements", **Journal of Information System Security**, 16 (1).
- Taylor, K.,& Maurer ,T.(2021)." Cyber Resilience and Financial Organizations: A Capacity-building Tool Box", **Carnegie Endowment for International Peace**, Available at:https://swiftinstitute.org/wp-content/uploads/2021/01/Guides_AR_fullse
- Tong, S.(2023).The Effectiveness of Information Disclosure under Cyber Attack. University of Miami Coral Gables, FL 33124 Available at:
https://aemps.ewapublishing.org/media/a6388e44283449d0a1953560ee2f01ba_OgnZqP9.pdf
- Tosun, O.K.(2021)."Cyber-attacks and stock market activity", **International Review of Financial Analysis** 76: 1-15.
- Vincent, N.E., Higgs, J.L. and Pinsker, R.E. (2019), "Board and management-level factors affecting the maturity of IT risk management practices", **Journal of Information Systems**, 33(6): 117-135.

ملحق 1: المؤشر المقترح للإفصاح عن مخاطر الأمن السيبراني

م	عناصر المؤشر
	أولاً: قنوات الاتصال الإلكتروني للشركة :
1	ماهية الشركة وطبيعتها.
2	الموقع الإلكتروني للشركة، البريد الإلكتروني، وسائل التواصل الرقمي الذي تعتمده الشركة، آلية التواصل مع أصحاب المصالح ذات الصلة.
	ثانياً: الإفصاح عن مخاطر الأمن السيبراني الفعلية والمحتملة:
3	سرقة أو فقدان البيانات (البيانات الشخصية، البيانات التجارية، أي بيانات ذات قيمة بالسوق) .
4	تدمير البيانات (مسح البيانات الإلكترونية، تشفير البيانات، منع الوصول إليها).
5	انقطاع الاتصالات (تعطيل الموقع الإلكتروني، تعطيل الشبكات، تشويه الموقع، الاستيلاء علي صفحات وسائل التواصل الاجتماعي).
6	القرصنة (إمكانية الوصول غير المصرح به إلي أنظمة الكمبيوتر والمعلومات المتصلة بالإنترنت أو التعديل، أو الاستغلال غير المشروع، أو سوء الاستخدام).
7	انتشار الفيروسات (إضافة برامج ضارة إلي نظام آخر بغرض تدمير النظام المهاجم).
8	سرقة الأموال والأوراق المالية والصناديق وغيرها.
9	المخاطر المتعلقة بانتهاك حقوق الملكية الفكرية، ومخاطر التصيد الاحتيالي.
	ثالثاً: الإفصاح عن الآثار المحتملة الناتجة عن حوادث الأمن السيبراني:
10	تعطيل النشاط/ تأخير التشغيل (زيادة المصروفات وانخفاض الإيرادات).
11	ضرر السمعة، الدعاوة القضائية، غرامات والتزامات، تعويضات ، انخفاض الميزة التنافسية.
12	التكاليف المدفوعة لتعزيز وحماية الأمن السيبراني في الشركة.
13	تكاليف التأمين المدفوع لشركات التأمين للحفاظ علي خصوصية الجهات الخارجية المتعاملة مع الشركة ضد أي هجوم سيبراني.
14	الإفصاح عن الخسائر المالية التي تترتب علي انتهاكات الأمن السيبراني بالشركة، انخفاض التدفقات النقدية المستقبلية
15	الإفصاح عن تكاليف الدورات التدريبية للعاملين لتعزيز وعيهم بشأن الانتهاكات السيبرانية
16	الإفصاح عن المبالغ المتكبدة للتعافي من الهجمات السيبرانية والإجراءات البديلة لضمان استمرار العمل في حالة حدوث هجوم سيبراني، وتقييم وتحسين إجراءات المخاطر السيبرانية.
	رابعاً: الإفصاح عن استراتيجيات الأمن السيبراني:
17	الإفصاح عن استراتيجيات وسياسات وإجراءات الأمن السيبراني في الشركة
18	الإفصاح علي أن الإدارة الأمنية السيبرانية تم انشائها وفق التشريعات والقوانين والتعليمات المتعلقة بحماية البيانات في الدولة.
19	الإفصاح عن تطبيق استراتيجيات التوعية والتدريب في مجال الأمن السيبراني للعاملين في الشركة للتخفيف من مخاطر الأمن السيبراني.
20	الإفصاح عن وجود إجراءات اتصال توفر معلومات عن الأمن السيبراني لمتخذي القرارات والعملاء والموظفين وأصحاب المصالح الآخرين في السوق والجهات التنظيمية.
21	لجنة استراتيجية إدارة مخاطر الأمن السيبراني
	خامساً: الإفصاح عن حوكمة إدارة مخاطر الأمن السيبراني:
22	الإفصاح عن مشاركة مجلس الإدارة في الإشراف والرقابة علي مخاطر الأمن السيبراني
23	الإفصاح عن وجود لجنة علي مستوي مجلس الإدارة مكلفة علي وجه التحديد بالأمن السيبراني. (لجنة المراجعة – لجنة إدارة المخاطر – لجنة التكنولوجيا)
24	الإفصاح عن ضوابط وإجراءات إدارة مخاطر الأمن السيبراني.
25	التقارير المرفوعة الي الإدارة العليا من قبل لجنة إدارة المخاطر عن حالات الاختراق والحوادث السيبرانية.

26	تقارير عن مشاركة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني.
27	تقارير عن مشاركة مستشار خارجي مستقل في التخفيف من مخاطر الأمن السيبراني.
28	تقارير عن مساهمة الإدارة في تصميم وتقييم نظام إدارة مخاطر الأمن السيبراني في الشركة، وآليات تعزيز وقدرة مواجهة المخاطر المستقبلية.
29	تقارير إجراءات الاستجابة للحوادث في نظم المعلومات والأمن السيبراني (خطة الطوارئ)، الإفصاح عن الخطط المستقبلية للحد من مخاطر الأمن السيبراني.
30	الإفصاح عن دليل استرشادي لمخاطر الأمن السيبراني.
	سادساً: الإفصاح عن حماية الأمن السيبراني:
31	إدارة الأصول السيبرانية، إدارة أمن الفضاء السيبراني، إدارة النسخ الاحتياطية. ضوابط علي الوصول غير المصرح به.
32	وجود برامج صد الهجمات السيبرانية وحماية الفضاء السيبراني تخضع للمراجعة من قبل قسم المراجعة السيبرانية.
33	الإفصاح الدوري عن الاستراتيجيات والسياسات والإجراءات المتبعة في حوكمة مخاطر الأمن السيبراني وتحديد المسئول عن حوكمة الأمن السيبراني.
34	الاستعانة بمتخصصين مؤهلين في مجال المخاطر الإلكترونية.
35	التدريب المستمر للعاملين لتعزيز وعيهم بشأن الانتهاكات السيبرانية.
36	التأمين ضد الحوادث السيبرانية.
37	الإفصاح عن خطة الاستجابة للتعافي من حوادث وانتهاكات الأمن السيبراني، واختبار خطة التعافي.
38	المراجعة المستمرة لجودة الخطط الاستراتيجية للحد من مخاطر الأمن السيبراني من قبل مجلس الإدارة.
39	تصميم وتفعيل هيكل الرقابة الداخلية للأمن السيبراني، واختبار الفعالية التشغيلية لضوابط رقابة الأمن السيبراني.
40	الالتزام بالتقرير عن النزاهة والأخلاق وفقاً لمعايير السلوك بالشركة، وتحديد معالجة الانحرافات، لدعم أداء برنامج إدارة مخاطر الأمن السيبراني.