

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة تطبيقية من البنوك المصرية المدرجة

د/ أحمد محمد علي أبو سمك

أستاذ المحاسبة المساعد

كلية التجارة – جامعة قناة السويس – مصر

كلية الأعمال - جامعة العين - العين - دولة الإمارات العربية المتحدة

المستخلص:

استهدف البحث معرفة أثر الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح من خلال دراسة تطبيقية على البنوك المصرية المدرجة، حيث تمثل مجتمع الدراسة في كافة البنوك المقيدة في سوق الأوراق المالية المصري والتي يبلغ عددها ١٢ بنك، خلال الفترة الزمنية من عام ٢٠١٨ حتى ٢٠٢٢ ، وتمثلت أهم نتائج البحث في وجود تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح العام عن الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح، ووجود تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح عن مخاطر الأمن السيبراني باستخدام القابلية للقراءة على استجابة أسعار الأسهم عقب إعلانات الأرباح، ووجود تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح عن مخاطر الأمن السيبراني باستخدام لغة التقاضي على استجابة أسعار الأسهم عقب إعلانات الأرباح. وتوصى الدراسة الحالية بضرورة توفير إطار عمل للإفصاح عن مخاطر الأمن السيبراني لكي يستطيع المستثمرون معرفة وضع المؤسسة تجاه مخاطر الأمن السيبراني.

الكلمات الدالة: الإفصاح عن مخاطر الأمن السيبراني، عوائد الأسهم، استجابة أسعار الأسهم، إعلانات الأرباح، لغة التقاضي ، القابلية للقراءة.

Abstract:

The research aimed to investigate the impact of disclosing cyber security risks on the response of stock prices to the announcement of profits through an applied evidence on listed Egyptian banks, as the study population represented all banks listed on the Egyptian stock market, 12 banks. The study sample starts from the year 2018 until the year 2022. The most important results of the research were the presence of a statistically significant direct effect of the levels of general disclosure about cyber security on the response of stock prices following earnings announcements. There is a statistically significant direct effect of the levels of disclosure of cyber security risks using readability on the response of stock prices following earnings announcements. There is a statistically significant positive effect of the levels of disclosure of cyber security risks using the language of litigation on the response of stock prices following earnings announcements. The current study recommends the need to provide a framework for disclosing cyber security risks so that investors can know the institution's position regarding cyber security risks.

Key Words: Cyber Security Risk Disclosure, Stock Returns, Stock Price Response, Earnings Announcements, Litigation, Readability.

١. المقدمة

تعرضت صناعة الخدمات المالية للهجوم السيبراني وفقاً لتقرير البنك الدولي في عام ٢٠١٨ أكثر من أي صناعة أخرى، وارتفعت تكاليف برامج الفدية في الولايات المتحدة إلى أكثر من ٨ مليارات دولار في عام ٢٠١٨ من ٢٥ مليون دولار في عام ٢٠١٤. اعتباراً من عام ٢٠٢١، استمرت الولايات المتحدة في تحمل أعلى تكلفة عالمية لكل اختراق للأمن السيبراني، مع ارتفاع التكاليف إلى ٨,٦٤ مليون دولار لكل حدث، إضافة إلى ذلك استغرق اكتشاف الاختراق واحتوائه ٢٨٠ يوماً في المتوسط (Jiang et al., 2022).

وفي عام ٢٠١١، أصدر قسم تمويل الشركات التابع للجنة الأوراق المالية والبورصة إرشادات الإفصاح عن الأمن السيبراني والتي تنص على أنه يجب على الشركات العامة أن تفصح في ملفاتها الخاصة بسوق الأوراق المالية عن مخاطر الحوادث السيبرانية التي تعد من بين أهم العوامل التي تجعل الاستثمار في الشركة محفوفاً بالمخاطر، وفي أعقاب اختراق Equifax لعام ٢٠١٧ واختراق قاعدة بيانات EDGAR لعام ٢٠١٧، وافقت هيئة الأوراق المالية والبورصات على إرشادات محدثة للشركات العامة لإعداد الإفصاحات عن مخاطر وحوادث الأمن السيبراني في عام ٢٠١٨. حيث تنص هيئة SEC صراحةً في توجيهاتها لعام ٢٠١٨ على أنه لا ينبغي للشركات استخدام المعلومات الخاصة غير المفصح عنها للتداول في الأوراق المالية للشركات المتضررة من انتهاكات الأمن السيبراني (Remeis, 2023).

يتمثل مفهوم الأمن السيبراني في حماية المعلومات الرقمية، فضلاً عن سلامة البنية التحتية ونقل المعلومات الرقمية، وبشكل أكثر تحديداً يشمل الأمن السيبراني مجموعة من التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به وذلك لضمان السرية والنزاهة والقدرة على الاستعادة. وتعد المخاطر السيبرانية موضوعاً مهماً جداً لجميع الشركات، بما في ذلك المؤسسات

المالية، وفي الواقع شهدت الشركات العاملة في صناعة الخدمات المالية أعلى تكلفة سنوية للجرائم، وفيما يتعلق بالبنوك فإن المخاطر السيبرانية هي مخاطر تتعلق بسلامة البيانات الإلكترونية (Smaili, et al.,2023)، وتشير دراسة (Harris, et al 2023) إلى أن البنوك تتعامل مع المخاطر المتمثلة في أن فشل نظام تكنولوجيا المعلومات قد يعيق أنشطتها اليومية.

١/١ فكرة البحث

تواجه الشركات مخاطر متزايدة تتعلق بالأمن السيبراني، حيث يمكن أن تؤدي الإختراقات السيبرانية إلى خسائر مالية كبيرة للشركات، ونظراً للآثار المالية والقانونية والسمعة الكبيرة للهجمات السيبرانية، فإن الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات العامة وكيفية إدارة هذه المخاطر أصبح ذات أهمية متزايدة بالنسبة للمستثمرين والحكومات والمستهلكين والبائعين وأصحاب المصلحة الآخرين لاتخاذ القرارات السليمة. ويمكن للشركات الحد من عدم التأكد بشأن مخاطر الأمن السيبراني وقياس عدم تماثل المعلومات مع أصحاب المصلحة الخارجيين من خلال الإفصاح المناسب عن مخاطر الأمن السيبراني (Remeis, 2023).

ويمكن أن يكون لاخترق أمن المعلومات تأثير اقتصادي سلبي، بما في ذلك انخفاض إيرادات المبيعات، ارتفاع التكاليف، انخفاض الأرباح، الأرباح المستقبلية، تدهور السمعة، انخفاض القيمة السوقية. ومع ذلك، يمكن أن تكون العواقب الاقتصادية طفيفة أيضاً على المدى الطويل لأن الشركات يمكنها حماية أصول المعلومات الرئيسية الخاصة بها (Arcuri, et al, 2018)، ولذا يعد فهم التأثير الحقيقي للهجمات السيبرانية على عوائد سوق الأوراق المالية أمراً بالغ الأهمية في تحديد مستويات الاستثمار في أنشطة أمن المعلومات.

حيث تعبر عوائد الأسهم عن نسب الأرباح المحققة من الاستثمار التي ينتظرها المستثمرون، من خلال قدرة أصول الشركة علي تحقيق دخل (Mall, & Gupta,

(2019)، وتعتمد كفاءة تخصيص أسواق رأس المال على مدى عكس أسعار الأصول الرأسمالية بشكل كامل للمعلومات التي تؤثر على قيمتها. ومع أخذ ذلك في الاعتبار، تمثل القيمة السوقية ثقة المستثمرين في الشركة، وقياسها هو وسيلة لحساب تأثير الهجوم السيبراني، كما أن سلوك المستثمر يعتمد على ما لاحظته في الماضي.

ويهتم المستثمرون بإعلانات الأرباح بشكل مرتفع ويوجد أدلة كثيرة تبين أن إعلانات الأرباح تحتوي على المعلومات التي تؤثر على أسعار الأسهم، ويعتقد كبار المسؤولين الماليين أن الأرباح هي أهم مقياس مالي يقدمونه للسوق، ووفقاً لذلك يتحمس المستثمرون للحصول على معلومات خاصة قبل إعلان الأرباح، مما يشكل توقعاتهم حول ما إذا كان من المحتمل أن ما تفصحه الشركة يساعدهم في تفسير المعلومات التي يتم الإفصاح عنها بالفعل وما إن كان البحث عن المعلومات بين أنواع عديدة من المشاركين في السوق (المحللين، المستثمرين، المؤسسيين) يساهم في رفع كفاءة السوق ويسهل عملية اكتشاف الأسعار (المر، ٢٠٢٢).

ويعكس الانحراف بعد إعلان الأرباح الصعوبة التي يتم بها تسعير أسعار الأسهم بشكل عقلائي فور صدور أخبار الأرباح بشكل غير متوقع في السوق بسبب الاهتمام المحدود الناتج عن القيود المعرفية للمستثمرين، وسوف تستمر العوائد اللاحقة في الانحراف لأعلى أو نحو الأسفل للحصول على أخبار جيدة أو سيئة، ولذلك يركز الانحراف بعد إعلان الأرباح عادةً على انتباه محدود للمستثمر، ومن ثم لا يستطيع المستثمرون معالجة جميع معلومات الإعلان واتخاذ قرارات استثمارية ملائمة عندما يتم إصدار إعلانات أرباح ضخمة في السوق، مما يؤدي إلى انخفاض رد فعل السوق حول تاريخ الحدث و الانحراف بعد إعلان الأرباح (Chen, et al., 2022).

فإذا أصدرت شركة إعلاناً متأخراً فمن الممكن أن تقوم المزيد من الشركات النظرية بالإعلان عن أرباحها، وسيكون لدى المستثمرين أيضاً المزيد من الوقت لدمج معلومات الشركات النظرية بشكل صحيح في معتقداتهم حول هذه الشركة، وبالتالي كلما تأخر إعلان أرباح الشركة المحورية، قلت المفاجأة في إعلان أرباحها، مما قد

يؤدي إلى انخفاض اهتمام السوق والتغطية الإعلامية. وفي المقابل، من خلال وجود استراتيجية إعلان مبكر، يمكن للشركات جذب المزيد من اهتمام السوق، الأمر الذي من الممكن أن يعزز ظهورها، ومن الممكن أن يحول اعتراف المستثمرين المكتسب من اهتمام السوق إلى فوائد طويلة الأجل للشركات (Truong, 2023).

وعلى ذلك فإن الإفصاح عن مخاطر الهجمات السيبرانية يؤثر سلباً على أسعار الأسهم، إضافة إلى أن الهجمات الناجحة التي يترتب عليها فقدان المعلومات المالية الشخصية للعملاء، توفر إشارات سلبية عن إدارة المخاطر السيبرانية للشركات المستهدفة وأصحاب المصلحة فيها والمنافسين مما يؤثر سلباً على سمعة الشركات، كما أن الهجوم السيبراني الناجح والذي ينتج عنه فقدان المعلومات المالية للأفراد والمنظمات، يقلل من ثروة المساهمين، وبناءً على ما سبق عرضه تتمثل فكرة البحث في قياس أثر الإفصاح عن مخاطر الأمن السيبراني على استجابة الأسهم للإعلان عن الأرباح.

حيث تتبع أهمية البحث من اهتمام الفكر المحاسبي بمخاطر الأمن السيبراني وتأثيرها على عوائد الأسهم، ومن اهتمام المنظمات المهنية والمستثمرين وزيادة وعي وإدراك معدي ومستخدمي التقارير المالية بتأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح في البنوك المقيدة ببورصة الأوراق المصرية خلال السلسلة الزمنية من ٢٠١٨ حتى ٢٠٢٢.

وبناء على ذلك يتمثل هدف البحث في قياس أثر الإفصاح عن مخاطر الأمن السيبراني على استجابة الأسهم للإعلان عن الأرباح، وتوضيح العلاقة بين مقاييس جودة الإفصاح عن الأمن السيبراني (عدد الكلمات، القابلية للقراءة، لغة التقاضي) على استجابة الأسهم للإعلانات عن الأرباح، وذلك من خلال عرض أهم ما توصلت إليه الأدبيات السابقة في مجال البحث من أجل تطوير الفروض البحثية، تمهيداً لاختبارها إحصائياً وعرض أهم ما توصلت إليه الدراسة الحالية من نتائج وتوصيات وأبحاث مستقبلية.

٢. الخلفية النظرية وتطوير الفروض البحثية في ضوء الأدبيات والإصدارات السابقة

2/1 التأسيس العلمي لمعلومات الأمن السيبراني : المخاطر والتهديدات

تعد الإدارة الفعالة للمعلومات أمر بالغ الأهمية يتضمن الاعتراف بنقاط الضعف المتزايدة، بما في ذلك التهديدات السيبرانية وحرب المعلومات، وفي هذا أشارت دراسة (Cheong et al., 2021) إلى أنه نظراً لانتشار استخدام المؤسسات لتكنولوجيا المعلومات وما يترتب عليها من ارتفاع في تهديدات الأمن السيبراني، فقد أصبح الأمن السيبراني قضية حيوية لكل المؤسسات، وذلك بغض النظر عن حجمها. وذكرت دراسة (Harris, et al, 2023) أن العديد من الصناعات تعتمد على الإنترنت، بما في ذلك الاتصالات السلكية واللاسلكية، والخدمات المصرفية والمالية وغيرها من الخدمات الحكومية الأساسية، وبما أن القطاعين العام والخاص أصبحا أكثر اعتماداً على التقنيات والشبكات القائمة على الويب في أنظمة الإدارة المالية الخاصة بهما، فقد أصبحا أكثر عرضة للتهديدات .

حيث أوضحت دراسة (Jackson et al., 2019) أنه في الفترة من عام ٢٠١٥ إلى عام ٢٠١٦، تضاعفت هجمات برامج الفدية أربع مرات لتصل إلى ٤٠٠٠ هجوم يومياً، كما ارتفع عدد اختراقات البيانات في الولايات المتحدة من ١,٠٩٣ مليوناً في عام ٢٠١٦ إلى ١,٥٧٩ مليوناً في عام ٢٠١٧ . وأشارت دراسة (Ponemon Institute, 2021) أنه في عام ٢٠٢١ ارتفع متوسط التكلفة الإجمالية لاختراق البيانات من ٣,٨٦ مليون دولار إلى ٤,٢٤ مليون دولار في الولايات المتحدة، وهو ما يعتبر أكبر زيادة من السنوات الماضية.

ووفقاً لما ورد بدراسة (متولى & غريب، ٢٠٢٢) فإنه غالباً ما يتم استخدام مصطلحات الأمن السيبراني وأمن المعلومات بالتبادل، حيث ذكرت الدراسة أن (AICPA, 2017) يصف الأمن السيبراني بأنه عملية تنفيذ وتشغيل الضوابط

وأشطة إدارة المخاطر الأخرى لحماية المعلومات والأنظمة من الأحداث الأمنية التي يمكن أن تعرضها للخطر عندما لا يتم منع الأحداث الأمنية، لاكتشاف، الاستجابة، التخفيف، والتعافي من تلك الأحداث في الوقت المناسب. كما تناولت الدراسة اختراقات الأمن السيبراني على أنها فقدان السرية أو النزاهة أو توافر المعلومات، بما في ذلك أي إعاقة ناتجة عن (١) تكامل المعالجة أو توافر الأنظمة أو (٢) نزاهة أو توفر مدخلات أو مخرجات النظام، والتي لها تأثير سلبي على تحقيق أهداف والتزامات أعمال المؤسسة (بما في ذلك التزامات الأمن السيبراني) وكذلك القوانين واللوائح المتعلقة بمخاطر الأمن السيبراني وبرنامج الأمن السيبراني.

وفي هذا السياق أشارت دراسة (Pacheco & Wheatley, 2022) إلى أن المخاطر الإلكترونية تتمثل في المخاطر المرتبطة بحدث إلكتروني خبيث قد يتسبب في تعطيل الأعمال التجارية وحدوث خسائر مالية، لذلك تهدف نظم إدارة المخاطر إلى تقييم المخاطر واتخاذ خطوات لتقليلها إلى مستوى مقبول، حيث تنقسم إدارة مخاطر الأمن السيبراني إلى تقييم المخاطر والتخفيف من حدة المخاطر، فبالنسبة إلى تقييم المخاطر يحدد المديرون المخاطر بناءً على البنية التحتية للمؤسسة، وبمجرد تحديد التهديدات والمخاطر يمكن للمديرين تجاهل المخاطر أو تخفيفها أو نقلها أو الاحتفاظ بها، بينما يتضمن التخفيف من حدة المخاطر اختيار وتنفيذ الضوابط الأمنية لتخفيضها إلى مستوى مقبول للإدارة، وقد تقوم الشركات أيضاً بتحويل المخاطر المالية عن طريق شراء تأمين متخصص، يوفر للشركة الأمان ضد المخاطر وعدم التأكد، ويساعد في تقليل احتمالية الخسارة المالية.

كما أشار (Deloitte, 2020) إلى أنه يمكن أن تكون المخاطر منتشرة، مما يؤثر على سلامة نظام المعلومات المالية بأكمله، أو تكون محددة مما يؤثر على التطبيقات الفردية أو قطاعات البيانات. وبغض النظر عن ذلك، فمن المحتمل أن تؤثر مخاطر الأمن السيبراني على الضوابط العامة وضوابط التطبيقات لنظام إعداد التقارير المالية، مما يزيد من احتمال حدوث أخطاء مادية (Smith et al., 2019). وفي سياق

اتفاق الأدبيات المحاسبية على مخاطر الأمن السيبراني فإن دراسة (Haapamäki & Sihvonen, 2019) قد أكدت على أن إطار إعداد التقارير الخاصة بإدارة مخاطر الأمن السيبراني يعد خطوة أولى حاسمة نحو تمكين حل متسق وقائم على السوق وقائم على الأعمال للشركات للتواصل بنجاح مع أصحاب المصلحة الرئيسيين حول كيفية إدارة مخاطر الأمن السيبراني.

وأشارت دراسة (Grove & Clouse, 2020) أن المعهد الأمريكي للمحاسبين القانونيين المعتمدين AICPA أنشأ دليل يركز على وصف الأمن السيبراني ومعايير التحكم حتى تقوم الشركات بتقييم مخاطر الأمن السيبراني، وفي هذا أشارت دراسة (Yang, et al. 2020) إلى أن (AICPA) طور إطار عمل لإعداد تقارير إدارة مخاطر الأمن السيبراني مكون من ثلاث أجزاء رئيسية من المعلومات تهدف إلى مساعدة أصحاب المصلحة في مراقبة برنامج إدارة مخاطر الأمن السيبراني للشركة وتوجيه الشركات في تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني، ويمكن استخدامه للإفصاح عن المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليتها.

ويعد صف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للشركة من المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة المخاطر السيبرانية وفعاليتها، حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة، وتزويد المستخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة، تأكيد الإدارة بشأن فعالية ضوابط الأمن السيبراني، وأنها تتوافق مع معايير AICPA وأن الضوابط التي تنفذها الإدارة يمكن أن تحقق أهداف الأمن السيبراني للشركة بشكل فعال، وتستند هذه الأهداف إلى مجموعة من معايير الرقابة المناسبة مثل معايير خدمات الثقة (الأمان، التوافر، السرية)، وأخيرا رأي المراجع في إفصاحات الإدارة وفعاليتها ضوابط الشركة ومنها(تقرير ضوابط النظام والتنظيم للأمن السيبراني).

كما أوضحت دراسة (Swift et al., 2020) أنه نتيجة لاختراقات الأمن السيبراني، يمكن أن تتعرض أصول الشركات ومعلومات العملاء للخطر، فضلاً عن التأثير على سمعتها، مما يؤدي إلى تكاليف علاج مرتفعة ومسؤولية قانونية محتملة، حيث يشعر أصحاب المصلحة بقلق متزايد بشأن الأمن السيبراني، وبالتالي يطالبون بمعلومات إضافية حول حوادث الأمن السيبراني، وتحديدًا تلك التي تتضمن على انتهاكات فعلية. وبحث دراسة (Andreadis, et al., 2022) في التكاليف غير المباشرة للسندات ومدى تأثير نشر المعلومات حول الهجمات السيبرانية من خلال مصادر إخبارية مهمة على سوق السندات، وأوضحت الدراسة أن العدد التراكمي للهجمات الإلكترونية التي تغطيها المقالات الإخبارية يؤثر سلباً بشكل كبير على عوائد السندات. كما قامت دراسة (Jensen and Paine 2023) بإجراء تحليل مماثل من خلال استخدام بيانات حول استثمار تكنولوجيا المعلومات، وهجمات برامج الأمن، والسندات، وأوضحت الدراسة أن عوائد السندات تتخضع تدريجياً مع الإفصاح عن الهجمات السيبرانية ويزداد الإنفاق على تكنولوجيا المعلومات.

كما ذكرت دراسة (Tsang, et al, 2023) أن مخاطر الأمن السيبراني يعد عاملاً مهماً عند الاستثمار، ويؤكد اتجاه كثير من الأبحاث على التأثير الاقتصادي الكبير لانتهاكات الأمن السيبراني على قيمة الشركة والسوق وذلك من خلال حدوث المخاطر الخارجية والمخاطر الداخلية، وانطلاقاً من مهمة حماية المستثمرين والهدف الضمني المتمثل في الحد من عدم تماثل المعلومات، تدعو لجنة الأوراق المالية والبورصة المستثمرين من خلال مطالبة الشركات العامة بالإفصاح عن المعلومات المالية ذات الدلالة وغيرها من المعلومات المادية ذات الصلة للجمهور.

وبناء على ما تناولته الأدبيات المحاسبية واتفاقاً مع ما ذكرته دراسة (علي، ٢٠٢٢) فإنه وبشكل عام يمكن تصنيف مخاطر التهديدات السيبرانية إلى ثلاثة أنواع رئيسية تتمثل في :

أولاً : المخاطر المالية والتشغيلية فقد تؤدي الحوادث السيبرانية إلى انخفاض التدفقات النقدية المستقبلية مما يؤدي إلى انخفاض قيمة بعض الأصول بما في ذلك الشهرة والأصول غير الملموسة المتعلقة بالعملاء والعلامة التجارية أو براءات الاختراع أو البرمجيات أو الأصول الأخرى طويلة الأجل المرتبطة بالأجهزة أو البرامج والمخزون (SEC, 2011). وبالنسبة للمخاطر التشغيلية يمكن أن تشمل الاحتيال والأمن وحماية الخصوصية والمخاطر القانونية والمخاطر المادية (مثل تعطيل البنية التحتية)، والمخاطر البيئية، وتؤثر المخاطر التشغيلية على رضا العملاء وسمعة الشركة وحقوق المساهمين مع زيادة المخاطر الشاملة للشركة.

ثانياً: مخاطر السمعة، والتي تتمثل في أنه قد يكون للهجمات الإلكترونية تداعيات وتأثيرات ترتبط بعلاقات المنشأة مع عملائها أو مورديها فمن المحتمل أن تلحق الهجمات السيبرانية الضرر بسمعة الشركة والسبب في ذلك أن الضرر يمكن أن يلحق بالعملاء فيصبحون ضحايا للهجمات السيبرانية لأن المعلومات المسروقة عادةً تعرض العملاء لسرقة الهوية أو حتى الخسائر المالية (DiStaso,2018) .

ثالثاً: مخاطر الامتثال ، حيث كان ظهور التهديدات السيبرانية حافزاً لمعظم الدول لوضع قوانين وقواعد صارمة للأمن السيبراني بهدف الحفاظ على سرية وسلامة وتوافر نظم المعلومات في الفضاء السيبراني، كما كانت الدافع الرئيسي وراء معظم الجهود التنظيمية، ويتطلب حماية الأمن السيبراني تنفيذ الضمانات أو الإجراءات المناسبة لمواجهة أي مخاطر تتعلق بالأمن السيبراني والتي منها إمتثال المنظمات بمتطلبات السلامة من خلال تدريب الموظفين والحصول على معدات الحماية المناسبة لحماية الأمن السيبراني، حيث يؤدي عدم الامتثال إلى تعرض المنشآت للدعاوى القضائية والإجراءات العقابية (Marotta & Madnick, 2020)

وحيث يترتب على تحقق مخاطر الأمن السيبراني حدوث العديد من التكاليف، فقد أشارت دراسة (Harris, et al, 2023) إلي أن التكاليف الإضافية المحتملة للهجوم السيبراني تشمل على تكاليف الإصلاح، بما في ذلك المسؤولية عن

الأصول والمعلومات المسروقة، وإصلاح الأنظمة التالفة، والحوافز المقدمة للعملاء وشركاء الأعمال لمنع فقدان الأعمال والحفاظ على العلاقات، وتكاليف حماية الأمن السيبراني، بما في ذلك التغييرات التنظيمية الكبيرة، التقنيات الجديدة، والتدريب، والاستشاريين الخارجيين، وتكاليف التقاضي والمسؤولية القانونية، بما في ذلك تلك التي تتحملها السلطات التنظيمية المحلية والوطنية والدولية، وزيادة أفساط التأمين، والضرر الذي يلحق بسعر سهم الشركة وقيمة المساهمين على المدى الطويل.

ولقد أشارت دراسة (Mazumder & Hossain,2023) إلى أن الإفصاح عن الأمن السيبراني يعد بمثابة أجنحة جديدة نسبياً لإفصاحات الشركات، ونظراً للطبيعة البارزة للهجمات السيبرانية على الشركات، فقد زاد الطلب على المعلومات المتعلقة بالأمن السيبراني والحاجة إلى تسهيل المحادثات القوية حول هذه المواضيع بشكل كبير عبر مجموعات أصحاب المصلحة الرئيسيين. فغالباً ما تسلط وسائل الإعلام الإخبارية الرئيسية الضوء على القلق بشأن الهجمات السيبرانية بسبب حدوث اختراقات الأمن السيبراني للشركات بشكل متكرر الأمر الذي يترتب عليه سرقة البيانات السرية للحصول على فوائد مالية سريعة وغير قانونية. ومن ثم، هناك طلب متزايد من أصحاب المصلحة لمزيد من الشفافية من الشركات العامة في كيفية تحديد المخاطر السيبرانية وقياسها وإدارتها. ولمعالجة هذا القلق المتصاعد، يجب على كل شركة ضمان حوكمة قوية للأمن السيبراني وتقديم إفصاحات كافية حول كيفية تحديد أولويات الأمن السيبراني وإدارته.

وتوضح دراسة (على ، ٢٠٢٢) أن الترابط الهائل بين أنظمة معلومات المنشأة وبين الأطراف على طول سلسلة التوريد كبايعين أو موردين أو شركاء أو عملاء أو موظفين أو أي طرف مرتبط بالمنشأة إلكترونياً يمكن أن يصبح نقطة ضعف يتسلل منها المهاجمون حيث قد يتمكن المهاجمون من التسلل بعمق إلى شبكات الشركات ومهاجمة طبقات مختلفة من الأنظمة بما في ذلك أنظمة تخطيط موارد المؤسسات (ERP) ودقتر الأستاذ العام، ونظراً للوظائف المركزية لنظم المعلومات

المحاسبية للشركة فمن المحتمل أن تشكل البيانات المخزنة على تلك الأنظمة ثروة ذات أهمية كبيرة لمجرمي الإنترنت، لذا يجب النظر في المخاطر المحتملة التي تأتي من تهديدات الأمن السيبراني لهذه البيانات.

حيث أوضحت دراسة (Kelton, & Pennington, 2020) أنه استجابةً للمخاوف من أن أصحاب المصلحة لا يتوافر لديهم المعلومات الكافية في التوقيت المناسب عن هجمات الأمن السيبراني ومخاطر هذه الهجمات على الشركات وكيفية إدارتها ، فقد اتجهت الهيئات المهنية والتنظيمية إلى تعزيز الإفصاح عن الأمن السيبراني ، وفي هذا الشأن أصدرت SEC مجموعة من الإرشادات بشأن إفصاح الشركات عن مخاطر الأمن السيبراني، توضح العوامل والإفصاحات الموصى بها بشأن المسائل الجوهرية والتي قد تتمثل في وقوع حوادث الأمن السيبراني السابقة ، واحتمال وحجم الأحداث المستقبلية للأمن السيبراني، وتكاليف التقاضي والمعالجة المرتبطة بحوادث الأمن السيبراني السابقة.

فقد صدر التوجيه الأول المتعلق بالتزامات الإفصاح المتعلقة بمخاطر الأمن السيبراني من قبل هيئة البورصة الأمريكية في عام ٢٠١١ لمساعدة الشركات في تقييم ما ينبغي أن تقوم به من إفصاحات في هذا الشأن إن وجدت، حيث نص ذلك التوجيه علي أنه في حالة عدم فرض متطلبات إفصاح صريحة مرتبطة بمخاطر الأمن السيبراني والحوادث الإلكترونية قد يتفق الإفصاح عن مخاطر الأمن السيبراني مع مشاركة المعلومات الجيدة في الوقت المناسب بهدف المساعدة في اتخاذ قرارات الاستثمار (Barry, et al, 2022) ، كما نص على أنه بالرغم من عدم وجود إلزام صريح بالإفصاح عن مخاطر الأمن السيبراني في الوقت الحالي، إلا أن عدداً من متطلبات الإفصاح قد تفرض التزاماً على المسجلين بالإفصاح عن مثل هذه المخاطر، وطبقاً للإرشادات يعتمد مستوى ونوع الإفصاح على ظروف الشركة بما في ذلك احتمالية وقوع حوادث إلكترونية وأثر ذلك الاحتمال على الشركة.

وفي عام ٢٠١٨ بعد حدوث العديد من الأختراقات قامت هيئة البورصة الأمريكية بتحديث وتوسيع إرشاداتها، بهدف تقديم المزيد من المساعدة للشركات في إعداد الإفصاحات عن مخاطر الأمن السيبراني، حيث يقوم هذا التحديث علي توضيح مدي التزام الشركات بالإفصاح عن مخاطر الأمن السيبراني والانتهاكات المادية والتأثير المحتمل لهذه الانتهاكات، وفي هذا الإرشاد تم التأكيد علي أهمية إجراءات الأمن السيبراني من خلال تناولها لأهمية إجراءات وضوابط الأمن السيبراني التي تمكن من الإفصاح عن مخاطر الأمن السيبراني بدقة في الوقت المناسب، كما تم إيضاح أن التداول من الداخل لحوادث الأمن السيبراني محظور حيث طالبت الإرشادات ضرورة الامتثال للشركات لقوانين التداول من الداخل فيما يتعلق بأي معلومات عن حوادث الأمن السيبراني، كما أكدت علي توفير الشركات لإجراءات وسياسات قائمة لمنع التداول بناءً على مخاطر الأمن السيبراني.

ونكرت دراسة (فرج، ٢٠٢٢) أن دليل إرشادات الإفصاح عن الأمن السيبراني الصادر عن هيئة البورصة الأمريكية يحتوي علي مجموعتين تتمثل المجموعة الأولى في قواعد مراجعة قواعد الإفصاح عن مخاطر الأمن وذلك من خلال سبع عناصر، يعبر العنصر الأول في المجموعة عن الأهمية النسبية التي من خلالها تقوم الشركات بالتركيز على مخاطر الأمن السيبراني عند إعداد تقاريرها السنوية، فيما يتمثل العنصر الثاني في عوامل المخاطرة بحيث ينبغي أن يحتوي إفصاح الشركات عن حوادث الأمن السيبراني الفعلية والمتوقعة علي المخاطر الخاصة بالإفصاح عن إدارة مخاطر الأمن السيبراني للمستثمرين؛ بينما يحتوي العنصر الثالث علي المركز المالي ونتائج الأعمال أي ألزمت الإرشادات الشركات بالإفصاح عن أي حوادث أمن سيبراني قد يكون لها تأثير جوهري علي المركز المالي ونتائج الأعمال. كما يناقش العنصر الرابع وصف طبيعة الأنشطة، وأوضحت الإرشادات الإجراءات القانونية في العنصر الخامس من المجموعة، وفي العنصر السادس أوضحت الإرشادات سياسات الإفصاح في القوائم المالية التي قد تتأثر بحوادث الأمن السيبراني سواء كانت من إيرادات أو مصروفات أو تدفقات نقدية، فيما أوضح العنصر السابع دور مجلس الإدارة بخصوص برنامج إدارة مخاطر الأمن السيبراني .

فيما احتوت المجموعة الثانية في هذه الإرشادات علي السياسات والإجراءات المتعلقة بالرقابة على الإفصاح عن إدارة مخاطر الأمن السيبراني ، ويتم تنفيذ ذلك من خلال التأكد من وجود تصميم جيد لضوابط وإجراءات الرقابة على برنامج إدارة مخاطر الأمن السيبراني المطبق بالشركة فهي جزء من أعمال لجنة المخاطر بالشركة، وضرورة التأكد من عدم استغلال الأطراف الداخلية لمعرفتهم بالأحداث الجوهرية المتعلقة بمخاطر الأمن السيبراني المطبق بالشركة فهي جزء من أعمال لجنة المخاطر بالشركة، وضرورة الإفصاح عن المعلومات المتعلقة بإدارة مخاطر الأمن السيبراني بشكل انتقائي وهي المعلومات غير المعلنة للمستثمرين.

وأشارت بعض الدراسات السابقة (Yang, et al. ,2020; Frank, et al , 2019) أن المعهد الأمريكي للمحاسبين القانونيين المعتمدين قد طور إطار عمل لإعداد تقارير إدارة مخاطر الأمن السيبراني لتوجيه الشركات في تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني، ويمكن استخدامها للإفصاح عن المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليتها، على وجه التحديد اقترح إطار العمل ثلاث أجزاء رئيسية من المعلومات تهدف إلى مساعدة أصحاب المصلحة في مراقبة برنامج إدارة مخاطر الأمن السيبراني للشركة تتمثل في وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني، تأكيد الإدارة بشأن فعالية ضوابط الأمن السيبراني، رأي المراجع في إفصاحات الإدارة وفعالية ضوابط الشركة ومنها(تقرير ضوابط النظام والتنظيم للأمن السيبراني).

وقد تشير حوادث الأمن السيبراني أيضاً إلى حالات فشل محتملة في الرقابة الداخلية ، وعلى ذلك تؤدي جودة الإفصاح عن مخاطر الأمن السيبراني إلى التأكد من دور الإدارة في تنفيذ الضوابط المناسبة لتهديد الأمن السيبراني وما إذا كانت الضوابط التي تم تنفيذها من شأنه أن يقلل من مخاطر التحريفات الجوهرية المستقبلية في البيانات المالية للعميل (Calderon& Gao ,2021). حيث تم التأكيد من قبل العديد من الدراسات (Masoud, & Al-Utaibi, 2022; Rosati, et al ,2020) على أهمية إعداد التقارير المالية عند تقييم الآثار المترتبة على حوادث الأمن السيبراني

والتي قد تشير إلى وجود أوجه القصور في إعداد التقارير المالية في المستقبل، وتوضح مؤشرات مخاطر الأمن السيبراني، وتجب على العديد من التساؤلات المرتبطة بكيفية تأثير الإفصاح عن مخاطر الأمن السيبراني على تقييم الشركة بسبب التغيير في تصورات المخاطر.

ويشير هذا الأمر بطبيعة الحال إلى أن مخاطر الأمن السيبراني في المؤسسات الكبرى يمكن إلى أن تسبب أضرار كبيرة بالشركات من حيث تكاليف العلاج والغرامات والسمعة لسنوات. فإذا كان الهجوم مباشراً على أنظمة المحاسبة، فقد يشير الحادث إلى مخاطر التلاعب بدفاتر وسجلات الشركة مما قد يؤثر على التقارير المالية، ولهذا فإن مدى استجابة السوق السلبية بعد الإعلان عن حادث إلكتروني يرجع إلى أن مثل هذا الحادث يشير إلى وجود نقاط ضعف جوهرية في الرقابة الداخلية، وفي هذا السياق فإن الآثار المحتملة لوجود ضعف في هيكل الرقابة الداخلية نتيجة للهجمات السيبرانية قد تؤثر بشكل سلبي على أسعار الأسهم عقب إعلانات الأرباح.

فقد وجدت دراسة (Chen.,et al ,2023) أن الإفصاح عن عامل الخطر يزيد من تصورات المستثمرين لمخاطر الشركة من خلال تقلب عوائد الأسهم في السوق، ويقلل من عدم تماثل المعلومات، كما وثقت الدراسة وجود ارتباط سلبي بين عوامل الخطر التي تم الإفصاح عنها والعوائد غير الطبيعية، مما يشير إلى قيام المستثمرين بدمج المعلومات من الإفصاح عن عوامل الخطر في سعر السهم. وتؤدي الإفصاحات الأكثر تحديداً عن عوامل الخطر إلى حركة أكبر لأسعار الأسهم وحجم التداول، مما يشير إلى أن الإفصاحات الأكثر تحديداً عن عوامل الخطر توفر فائدة أكبر للمستثمرين.

وبناء على ذلك فإن الإفصاح عن الأمن السيبراني قد يتمثل في توفير معلومات دقيقة لأصحاب المصلحة حول مستوى ونطاق مخاطر الأمن السيبراني، فقد أشارت دراسة (Li et al., 2018) أن الإفصاح عن مخاطر الأمن إلزامي، إلا

أنه قد يكون غامضاً أيضاً. حيث تقوم الإدارة بصياغة الإفصاحات بشكل استراتيجي، مع الأخذ في الاعتبار التكاليف والحوافز المحتملة، فقد فرضت الهيئات التنظيمية ضغوطاً متزايدة على الشركات التي تفشل في تقديم الإفصاحات المناسبة عن مخاطر الأمن السيبراني، ولهذا يعد فهم الإفصاح عن مخاطر الأمن السيبراني أمراً بالغ الأهمية، لأنه يمكن أن يساعد المستثمرين على تقييم مخاطر الأمن السيبراني للشركة وتزويد المنظمين بمعلومات حول ما إذا كانت هناك حاجة إلى قواعد تشريعية إضافية.

٢/٢ استجابة أسعار الأسهم للإعلان عن الأرباح: سياق محاسبي

تميل الإعلانات المبكرة للأرباح إلى الحصول على اهتمام متزايد من السوق، والتغطية الإعلامية لأنها تحتوي على معلومات أكثر حداثة، حيث يستخدم المستثمرون والمحللون هذه الإعلانات لاستنتاج معلومات ليس فقط عن الشركات المعلنة ولكن أيضاً عن ظروف الصناعة والسوق، ولذلك يسمح المعلنون للمشاركين في السوق بتحديث توقعاتهم بشأن الشركات التي تعلن متأخرة، مما يؤثر على كمية المعلومات الجديدة التي يتم الإفصاح عنها عندما يعلن المعلنون المتأخرون بالفعل عن أرباحهم (Truong, 2023).

كما يترتب على الإعلان عن توزيعات الأرباح سواء زيادة أو نقص معلومات إيجابية أو سلبية عن قيمة الشركة، وهذا يؤثر على أداء الأسهم بشكل كبير ولذلك عادةً تستجيب الأسواق المالية بقوة للإعلان عن تخفيض توزيعات الأرباح مقارنةً بالإعلان عن زيادة توزيعات الأرباح (Hasan, et al, 2023)، فعندما يتم الإعلان عن الأرباح، يقوم كل مستثمر بتقييم ما إذا كانت المعلومات الواردة في الأرباح المعلنة تغير ملكية المستثمر المرغوبة لأسهم الشركة، حيث تحتوي الأرباح على مكونات ذات آثار مختلفة على قرارات المستثمرين الاستثمارية سواء كانت شراء أسهم الشركة أو الاحتفاظ بها أو بيعها وبأي سعر، ولكن عندما تكون الأرباح في الوقت المناسب بشكل غير متماثل، يجب على المستثمرين أيضاً تحديد ما إذا كانت أرباح

الشركة تتعلق بالأخبار الجيدة أو السيئة، وقد يؤدي عدم تماثل التوقيت إلى وجود اختلافات أكبر بين الأخبار الجيدة والسيئة وهذا يؤثر على الأرباح وعلي قرارات الاستثمار (Barth, et al., 2020).

حيث يعتمد رد فعل أسعار الأسهم للتغير في الأرباح على خصائص الشركة وخصائص توزيعات الأرباح، فعندما يكون تغيير توزيعات الأرباح كبيراً يكون رد فعل أسعار الأسهم قوي، وعندما يكون عائد توزيعات الأرباح مرتفع يكون توزيع الأرباح النقدية مرتفع، ومن ضمن هذه الخصائص أن يكون حجم الشركة صغير، الربحية مرتفعة، أو الملكية المؤسسية منخفضة، ومن ثم يجب على المستثمرين الذين لديهم معلومات أن يكونوا أكثر اهتماماً باستغلال هذه التغيرات في توزيعات أرباح الأسهم عند اتخاذ قراراتهم الاستثمارية (Asem, 2022).

كما توجد عدة عوامل تزيد من القيمة السوقية للأسهم وترتبط بتوزيعات الأرباح منها تحسين الوضع المالي للشركة ونمو أرباحها نظراً لاحتوائه على نمو توزيعات الأرباح وعائد الأسهم أيضاً، كما تعد الاحتياطات المالية للشركة من ضمن هذه العوامل لكونها بمثابة ضمان لتوزيع الأرباح ومصدر لزيادة رأس المال، بالإضافة إلي المعاملات المالية للشركة كالاندماج مع شركة أخرى أو الاستحواذ عليها والإعلان عن إصدار جديد للأسهم أو إصدار السندات (Temirov, et al, 2023).

وفي هذا السياق قامت دراسة (Chatterjee & Tiwari, 2022) بتحليل رد فعل أسعار الأسهم تجاه الإعلان عن تخفيض توزيعات الأرباح في سوق الأسهم الهندية والرقابة على عمليات إعادة شراء الأسهم، وذلك خلال الفترة 2009-2019 وبلغت عينة الدراسة 500 شركة مدرجة، وأظهرت نتائج الدراسة أن الإعلان عن تخفيض توزيعات الأرباح يؤثر سلباً على العوائد غير العادية حيث تلجأ الشركات التي تواجه رد فعل سلبي على أسعار الأسهم بعد الإعلان عن تخفيض توزيعات الأرباح إلى إعادة شراء الأسهم في نفس العام لتعزيز أسعار الأسهم، كما يؤدي

الإعلان عن تخفيض توزيعات الأرباح المرحلية إلى ردود فعل سلبية على أسعار الأسهم أكثر من الإعلان عن تخفيض توزيعات الأرباح النهائية.

وأشارت دراسة (الم، ٢٠٢٢) إلى أن الإعلان عن الأرباح ينقسم إلى ثلاث أنواع متميزة تتمثل في الإعلان عن الأرباح الجيدة ويحدث عندما يكون الربح الفعلي أكبر من الأرباح المقدر، والإعلان عن الأرباح المحايدة الذي يحدث عندما يتساوى الربح الفعلي مع الأرباح المقدر، وأخيراً الإعلان عن الأرباح السيئة ويحدث هذا عندما يكون الربح الفعلي أقل من الربح المقدر، فقد يتعين علي المديرين الإفصاح عن التقارير المالية مثل إعلان الأرباح كإشارة فعندما يكون إيجابي يؤدي إلي زيادة عوائد الأسهم وعندما يكون سلبي يترتب عليه انخفاض في عوائد الأسهم.

وأشارت دراسة (Martins, 2022) إلى أن إعلانات الأرباح تحمل معلومات مهمة عن الشركات، فقد تناولت نظرية Modigliani-Miller أن القيمة السوقية للشركة يتم حسابها بشكل صحيح على أنها القيمة الحالية لأرباحها المستقبلية وأصولها الأساسية، وباعتبارها مستقلة عن هيكل رأس المال الخاص بها، كأحد العناصر الرئيسية لتشكيل السعر "العادل" لأسهم الشركة، ومن الطبيعي أن إعلانات الأرباح قد تغير الصورة الكاملة حول مستقبل الشركة أو ببساطة تؤكد التوقعات السابقة، وفي بعض الحالات قد يستمر رد الفعل الأولي لإعلانات الأرباح عدة أسابيع أو حتى أشهر، وتسمى هذه الحالة بالانحراف بعد إعلان الأرباح (PEAD)، ويدل الانحراف في سعر سهم الشركة علي اتجاه مفاجئ لأرباح الشركة لفترة طويلة من الزمن.

وأوضحت نتائج دراسة (Chatterjee et al.2021) أن الإعلان عن توزيعات الأرباح النقدية ينتج عنها عوائد غير عادية على الأسهم مباشرة بعد الإعلان ولكن ذلك التأثير لفترة قصيرة جداً، ثم تعود أسعار الأسهم إلى طبيعتها تدريجياً، حيث يفضل المستثمرون مكاسب رأس المال على توزيعات الأرباح النقدية بسبب العيوب الضريبية المرتبطة بدخل الأرباح النقدية، ومن ثم فإن توزيعات الأرباح من قبل الشركات لا تؤثر على قرارات المستثمرين بشأن الاستثمار في الأسهم.

وأوضحت دراسة (Truong, 2023) أنه وفقاً لنظرية الإفصاح التنافسي فإن التأثيرات التكميلية للأدلة في توقيت إعلان الأرباح ، حيث تفترض النظرية أنه بما أن المستثمرين لا يستطيعون الاهتمام بجميع الشركات ، فإن الشركات لديها الحوافز لإنفاق المزيد من الموارد على الإفصاح للتنافس على جذب انتباه المستثمرين. وفي سياق إعلان الأرباح يمكن للشركات التنافس على الاهتمام من خلال اختيار موعد الإعلان عن أرباحها. فقرار الإعلان عن الأرباح في وقت مبكر يحتوي على مقايضة فمن الممكن أن يشهد المعلنون الأوائل الذين يجذبون المزيد من اهتمام المستثمرين زيادة في اعتراف المستثمرين، مما قد يكون له آثار إيجابية على كفاءة أسعارهم ، بالرغم من احتمالية تحملهم تكاليف إضافية.

ووفقاً لفرضية السوق الكفاء (EMH) يجب دمج جميع المعلومات بالكامل في أسعار الأسهم ، فغالباً ما تحلل بعض الدراسات الحالية (Hsu,& Chen, 2020المر، ٢٠٢٢) استجابات أسعار الأسهم لإعلانات الأرباح وتستند إلى تأثيرات PEAD & ERC لفحص الاختلافات في كفاءة معلومات السوق، حيث يمثل ERC العلاقة بين عوائد الأسهم والأرباح غير المتوقعة ، أي حساسية استجابات السوق لمفاجآت الأرباح، بينما تمثل PEAD استجابة الأسهم المتأخرة أو رد فعل السوق على أخبار الأرباح فإذا زادت كفاءة معلومات السوق ، فمن المتوقع أن تتسارع تصحيحات الأسعار الناتجة عن أخبار الأرباح وتتركز بشكل أكبر حول فترات الإعلان (أي زيادة عوائد الأسهم والأرباح غير المتوقعة).

وتتمثل النقطة المرجعية لتقسيم توزيعات الأرباح في عدة عوامل كمستويات الأرباح السابقة وتوقعات السوق، وتؤثر تلك النقطة المرجعية على سياسة توزيع الأرباح بشكل كبير حيث يهدف المديرون إلى تجنب النتائج أو الخسائر السلبية عن طريق الحفاظ على مستوى توزيع الأرباح الحالي أو زيادته، ولذلك يقوم المديرون بملائمة قراراتهم مع تلك النقطة المرجعية، ففي فترات الركود الاقتصادي يمكن أن يؤثر تجنب الخسارة على سياسة توزيع الأرباح ، وقد يتردد المديرون في تخفيض

أرباح الأسهم بسبب محاولة تجنب الخسارة وذلك لتجنب التوقعات السلبية والحفاظ على تقييم الشركة، نظراً لاعتقاد المستثمرين بأن حدوث أي تغييرات لتوزيعات الأرباح تعد مؤشر لمخاطر الشركة (Hasan, et al,2023).

٢/٢/١ محددات تقلبات عوائد الأسهم

تعتبر عوائد الأسهم عن التدفقات النقدية التي تعود على المستثمر نتيجة تحمله لمخاطر الأسهم لفترة زمنية معينة، ولذلك يهتم المستثمرون بعوائد الأسهم المتوقعة للشركة، ولكونها تساعد في التنبؤ بمستقبل الشركة مما يساعدهم على اتخاذ القرارات، فهي رقم محاسبي يعبر عن العديد من المعلومات المفيدة للمستثمرين، ولهذا طالبت معايير المحاسبة بالإفصاح عن نصيب كل مساهم من صافي ربح الشركة في قائمة الدخل، نظراً لتعبير الربح المحقق للأسهم عن مقاييس الربحية الجيدة التي يمكن من خلالها قياس الأداء ومن ثم الحصول على المعلومات الهامة للتحليل المالي (Kumar, et al. 2022).

كما أشارت دراسة (Sun, et al, 2022) إلى أن تقلبات عوائد الأسهم تنتج عن المخاطر التي يواجهها المستثمرون في أسواق الأسهم العالمية، ويصعب قياس تلك التقلبات بسبب تعدد وتنوع العناصر التي تؤثر في حركة الأسواق، كما يوجد العديد من العوامل التي تؤثر في حركة الأسعار بالسوق ومنها عوامل تتعلق بالمستثمرين والمتداولين بالسوق، عوامل إقتصادية، عوامل تتعلق بالقطاع الذي تصنف فيه الشركة أو بالشركة المدرجة التي تصدر الأسهم (Teodosio, et al,2022)، ويتضح من ذلك وفي ذات السياق أن تقلبات عوائد الأسهم تعد مؤشر سلبي على قيمة الشركة ومدى استمرارها في السوق ومن ثم قد يترتب عليها زيادة مخاطر الشركة، ولذلك فهي تعتبر مصدر خطر وقلق لأي مستثمر

وقد ناقش معيار المحاسبة الأمريكي (SFA.28) القياس والإفصاح عن عوائد الأسهم، كما طالب بالإفصاح عن عوائد الأسهم في حالة هيكل بسيط لرأس المال، وبالعرض المزدوج لعوائد الأسهم الأساسي والمخفض في قائمة الدخل للشركة التي لديها هيكل مركب لرأس المال، ووضح المعيار أيضاً كيفية احتساب عوائد

الأسهم الأساسية من خلال قسمة الدخل المتاح لحملة الأسهم على المتوسط المرجح لعدد الأسهم العادية القائمة خلال الفترة، وبالنسبة لعوائد الأسهم المخفضة التي تعكس التخفيض المحتمل لعوائد الأسهم التي يمكن أن تحدث إذا تم تحويل الأوراق المالية إلى أسهم عادية (McEnroe, & Mindak, 2020).

وعرض معيار المحاسبة الدولي رقم (IAS33) كيفية قياس عوائد الأسهم الأساسية عن طريق قسمة صافي ربح الفترة أو خسارتها المنسوب لحملة الأسهم العادية بعد خصم أرباح الأسهم الممتازة على متوسط عدد الأسهم العادية خلال الفترة، كما تناول المعيار طريقة احتساب عوائد الأسهم المخفضة عن طريق تعديل صافي الربح المنسوب لحملة الأسهم العادية والمتوسط المرجح لعدد الأسهم العادية القائمة بتأثيرات جميع الأسهم العادية المحتملة، بالإضافة إلى مطالبة المعيار بضرورة عرض الشركات لعوائد الأسهم الأساسية والمخفضة في متن قائمة الدخل لكل فئة من الأسهم العادية التي لها حق مختلف للمشاركة في صافي ربح الفترة، وهذا بدوره ساعد على قابلية مقارنة القوائم المالية (van Zyl, & Uliana, 2022).

وتعد تقلبات عوائد الأسهم قضية هامة في سوق الأوراق المالية فهي تجذب اهتمام كبير من قبل المستثمرين، وتعرف تقلبات عوائد الأسهم بتذبذب أسعار وعوائد الأسهم كما تمثل تلك التقلبات مقياس للمخاطر التي يواجهها المستثمرين، وتشير تقلبات عوائد الأسهم إلى عدم تماثل المعلومات، وتدل تقلبات عوائد الأسهم على مواجهة الشركة لمخاطر أعلى ومن ثم زيادة تكلفة رأس المال الشركة، لذا تعد تقلبات عوائد الأسهم مؤشر سلبي لقيمة الشركة ويوجد العديد من العوامل التي تؤثر على تقلبات عوائد الأسهم (المر، ٢٠٢٤).

وأوضحت دراسة (Khan, et al.2020) أن زيادة توزيعات الأرباح يترتب عليها خفض تقلبات أسعار الأسهم، حيث أكدت الدراسة على وجود علاقة إيجابية غير ذات أهمية بين عوائد الأرباح وتقلبات أسعار الأسهم، كما أشارت إلى أن سياسة توزيع الأرباح ليست في حد ذاتها العامل الوحيد المحدد لتقلبات الأسعار، وذكرت

الدراسة أن هناك بعض العوامل الأخرى التي تساهم في قياس تقلبات أسعار الأسهم، فقد يرتبط حجم الشركة سلباً بتقلبات أسعار الأسهم، كما أن الشركات ذات القيمة السوقية المرتفعة أفضل في إدارة تقلبات أسعار أسهمها مقارنة بنظيراتها، بالإضافة إلى تمتع الشركات ذات الخبرة بالكفاءة في إدارة أسعار أسهمها ويرتبط عمر الشركة سلباً بتقلبات أسعار الأسهم.

وترى الدراسة الحالية أن أهم العوامل التي تؤثر في تقلبات الأسهم تتمثل في جودة الأرباح، الإفصاح المحاسبي، المعلومات المستقبلية، حيث تعددت الدراسات التي تناولت العلاقة بين جودة الأرباح وعوائد الأسهم حيث أن الشركات ذات جودة أرباح منخفضة لديها تقلبات أعلى في عوائد الأسهم، ونظراً لتأثر جودة الأرباح بممارسات إدارة الأرباح إذ أن ممارسات إدارة الأرباح الحقيقية تمنع السوق من تقييم الأرباح المستقبلية للشركات التي تنعكس على عوائد الأسهم الحالية (Jeong, & Choi, 2019).

بينما أظهرت دراسة (Fonou-Dombeu, et al., 2022) أن الشركات ذات القيمة العالية لجودة أساس الاستحقاق وتلك ذات الأرباح المستمرة تكون ذات تقلبات منخفضة في عوائد الأسهم، وأشارت أيضاً إلى أن الشركات ذات الأرباح الأقل تواجه زيادة في تقلبات عوائد الأسهم. وقد تتأثر عوائد أسهم البنوك التي لديها محتوى معلوماتي أعلى ومخاطر أقل حيث ترتبط بوجود بيئة معلومات أكثر شفافية، فالإفصاحات المحاسبية لها تأثير كبير ومرتبطة بالقيمة السوقية لسعر السهم للقطاع المالي وخاصة البنوك التجارية.

وتناولت بعض الدراسات العلاقة بين عوائد الأسهم والمعلومات المستقبلية كدراسة (Widiastuti, et al. 2022) التي توصلت إلى أن الإفصاح عن المعلومات المستقبلية لم يؤثر على قيمة الشركة، بالرغم من إن أداء الشركة له تأثير إيجابي على قيمة الشركة، وأشارت الدراسة إلى أن التفاعل بين أداء الشركة والمعلومات المستقبلية يؤثر بشكل إيجابي على قيمة الشركة، وعلى العكس من ذلك قد يكون للمعلومات المستقبلية المالية تأثيرات كبيرة على أسواق رأس المال نظراً لأن تقلبات

الأسهم مرتبطة بعدم تماثل المعلومات وبزيادة مخاطر الشركة ، فالمعلومات المستقبلية التي تم الإفصاح عنها من قبل الشركات ذات السمعة العالية لها تأثير أكبر على قلب عوائد الأسهم، وتوصلت دراسة (Anwar, et al.,2021) إلي أن مستوى الإفصاح وجودته عن المعلومات المستقبلية قد يرتبط بشكل كبير بعوائد الأسهم للشركة في ظل نموذج عوائد الأرباح.

٢/٣ مقاييس جودة الإفصاح عن مخاطر الأمن السيبراني في ضوء استجابة الأسهم لإعلانات عن الأرباح

بحثت دراسة (Lending, et al. 2018) في قياس التغيرات في عوائد الأسهم بعد اختراق البيانات، وأوضحت أن التأثير المالي للاختراق واضح على المدى الطويل، حيث تواجه البنوك التي تتعرض لاختراقات البيانات انخفاضات كبيرة في الودائع، وأن المؤسسات غير المصرفية تواجه انخفاضات كبيرة في المبيعات على المدى الطويل. وأكدت دراسة (Tosun , 2021) علي تفاعل الأسواق المالية مع الاختراقات الأمنية غير المتوقعة للشركات على المدى القصير والطويل، حيث أوضحت أن رد فعل السوق من حيث حجم التداول والسيولة وضغوط البيع حيث يتوقع حدوث تغيرات سلبية في أسعار الأسهم، والتي يتبين أنها كبيرة وسلبية فقط في اليوم التالي للإفصاح العلني عن الاختراقات الأمنية، كما أن الاختراقات الإلكترونية تؤثر على سياسات الشركات على المدى الطويل، وهذا يعني أن الاختراقات الأمنية تمثل صدمات سلبية غير متوقعة لسمعة الشركات.

وذكرت دراسة (Celeny, & Maréchal, 2023) أن مخاطر أمن المعلومات تؤثر على عوائد الأسهم من خلال حساب العوائد غير العادية التراكمية في حالة صدور تقارير بالصحف عن حوادث الأمن السيبراني، فالأخبار المتعلقة بمخاطر أمن المعلومات لها تأثير ذو دلالة إحصائية على عوائد أسهم الشركات المتداولة علناً. كما ناقشت الدراسة أن العوائد التراكمية غير العادية حول أحداث الأمن السيبراني في الشركات المتداولة علناً في الولايات المتحدة خسرت في المتوسط ٣٧,٠% من قيمة

أسهمها عند حدوث اختراق للبيانات، حيث تساهم المخاطر الناتجة عن الاحتيال في بطاقات الدفع بشكل أكبر في عوائد الإفصاحات السلبية مقارنة بأنواع الاختراقات الأخرى، وتكون التأثيرات السلبية أكثر أهمية بالنسبة للشركات التي لديها انتهاكات للبطاقات أكبر من المتوسط.

فقد بحث عدد قليل من الدراسات العوامل التي تدفع إلى مستويات أعلى من الإفصاح عن مخاطر الأمن السيبراني، فتناولت دراسة (Jiang, et al, 2022) ما إذا كانت الشركات تغير من إفصاحها عن الأمن السيبراني بعد حدوث اختراق للأمن السيبراني، وتوصلت الدراسة إلى أن ردود أفعال السوق تؤثر على سلوك الإفصاح عن الأمن السيبراني للشركات بعد الاختراق. وأفادت دراسة (Calderon & Gao, 2022) أن الشركات تغير سلوك الإفصاح الخاص بها بعد تلقيها خطاب تعليق من هيئة الأوراق المالية والبورصات حول الإفصاح عن مخاطر الأمن السيبراني الخاصة بها. وبالمثل، وثقت دراسة (Wang, et al, 2022) أن الشركات التي تلقت خطابات التعليق غيرت سلوكيات الإفصاح الخاصة بها كما هو مطلوب من قبل هيئة الأوراق المالية والبورصات.

وفحصت دراسة (Wang, et al., 2022) رد فعل السوق على خطابات تعليقات هيئة الأوراق المالية والبورصات المتعلقة بإفصاحات الأمن السيبراني، وأشارت الدراسة إلى أن السوق يتفاعل بشكل سلبي مع الردود التي تقدمها الشركات العامة إلى هيئة الأوراق المالية والبورصات بعد تلقي رسائل تعليق حول الكشف عن مخاطر الأمن السيبراني الخاصة بهم، هذا وتناقش الأدبيات السابقة عدة مقاييس لجودة الإفصاح عن مخاطر الأمن السيبراني مثل: عدد الكلمات، القابلية للقراءة، لغة التقاضي، ويمكن للدراسة توضيح العلاقة بين هذه المقاييس وعلاقتها باستجابة الأسهم لإعلانات الأرباح.

٢/٣/١ مقياس عدد الكلمات وعلاقته باستجابة الأسهم لإعلانات عن الأرباح

أشارت دراسة (Cao, et al., 2023) إلى أن اختراقات البيانات مكلفة للشركات المتضررة، مما يضر بسمعتها، ويقلل المبيعات، بل ويؤدي إلى خسارة الأعمال، وتؤدي هذه الحوادث أيضاً إلى تدهور التصنيف الائتماني للشركات وتجعل تدفقاتها النقدية أكثر تقلباً. ومن الممكن أن يكون مديرو الشركات حساسين للآثار السلبية للإفصاح عن اختراقات البيانات على سمعتهم، وسلامتهم الوظيفية، ومخصصاتهم المالية، ومن ثم قد يقومون بتخزين أخبار سيئة حول انتهاكات البيانات أو توقيت إفصاحاتهم بشكل استراتيجي للتخفيف من العواقب، ومع ذلك عندما تصل الأخبار السيئة المتراكمة إلى مستوى خطر لا يمكن للمديرين إخفاءها لفترة أطول وسيتعين عليهم الإفصاح عن مثل هذه الأخبار، مما قد يؤدي إلى انهيار أسعار الأسهم، وهو أمر سلبي كبير في توزيع عوائد الأسهم (Foerderer, & Schuetz, 2022).

وبحثت دراسة (Gao et al. 2020) في الاتجاه المتزايد على المدى الطويل في المحتوى والخصائص اللغوية للإفصاح عن مخاطر الأمن السيبراني للشركات العامة ويقدم نظرة ثاقبة للعوامل التي قد تدفع هذه الاتجاهات. حيث تظهر نتائج الدراسة أن أكثر مخاطر الأمن السيبراني التي تم الإفصاح عنها هي مخاطر انقطاع الخدمة/التشغيل ومخاطر انتهاكات البيانات، وكان لتوجيهات هيئة الأوراق المالية والبورصات لعامي ٢٠١١ - ٢٠١٨ تأثيرات إيجابية على طول مدة الإفصاح عن مخاطر الأمن السيبراني، وتشمل العوامل الأخرى التي أدت إلى الاتجاه المتزايد في الإفصاحات نوع الصناعة، ومخاطر الأمن السيبراني الشاملة في البيئة العامة، وحجم الشركة، وحوادث اختراق الأمن السيبراني السابقة.

وفي هذا السياق استخدمت دراسة (Cheong, et al 2021) مزيجاً من تحليل المحتوى وتحليل العوامل لتصنيف الإفصاحات عن مخاطر الأمن السيبراني إلى فئات عوامل خطر مختلفة. ووجدت الدراسة أن الشركات لديها أنماط إفصاح مختلفة اعتماداً على ما إذا كانت قد تعرضت لحوادث تتعلق بالأمن السيبراني أو نقاط ضعف في الرقابة

الداخلية. كما تسعى بعض الدراسات إلى استكشاف عواقب الإفصاح عن مخاطر الأمن السيبراني، حيث بحثت دراسة (Berkman, et al., 2018) فيما إذا كان الوعي بالأمن السيبراني الذي يتم قياسه بواسطة مؤشر الإفصاح يرتبط بتقييم السوق، ووجدت الدراسة أن السوق يقدر بشكل إيجابي الوعي بالأمن السيبراني وأن النغمة الأكثر سلبية في الإفصاحات السيبرانية ترتبط بانخفاض قيم السوق.

وقد ينقل الإفصاح عن اختراق الأمن السيبراني معلومات مفيدة للمستثمرين في تقييم الشركات الأخرى غير المخترقة في نفس الصناعة، ويوجد ثلاثة احتمالات لردود فعل المستثمرين : أولاً، قد ينظر المستثمر إلى اختراق الأمن السيبراني باعتباره أمراً خاصاً وفي هذه الحالة سيقوم المستثمرون بتعديل وجهة نظرهم تجاه الشركة المخترقة ولكنهم لن يقوموا بإجراء أي تعديلات على القيمة السوقية للشركات المنافسة (Kelton, & Yang, 2023). ثانياً، يجوز للمستثمرين النظر إلى انتهاك الأقران باعتباره معلومات إيجابية للشركات المنافسة وهذا ما يعرف بتأثيرات المنافسة، حيث يتمكن المنافسون في الصناعة من الحصول على حصة سوقية من الشركة المخترقة مما يؤدي إلى رد فعل إيجابي في السوق للشركات . ثالثاً، قد يعتبر المستثمرون انتهاك الأقران بمثابة معلومات سلبية عن الشركات المنافسة، مما يدفع المستثمرين إلى تعديل القيمة السوقية لهذه الشركات التي لم يتم اختراقها سيبرانياً (Kelton, & Yang, 2023).

وقد أشارت دراسة (Jackson et al., 2019) إلى أن المستندات الأطول في الإفصاح عن مخاطر الأمن السيبراني تُستخدم كأداة لإخفاء الأخبار السلبية (قد تحاول الإدارة إخفاء الأخبار السيئة عن أصحاب المصلحة عن طريق إخفائها في مستندات أطول، عندما يصبح حجم المستند أكبر، تصبح إمكانية قراءة المستند أكثر صعوبة) ، الأمر الذي قد يؤدي إلى حدوث انحراف بعد إعلان الأرباح .

كما أشارت دراسة (Chen, et al., 2022) إلى أن الانحراف بعد إعلان الأرباح (PEAD) يعد مشكلة أساسية حيث تصف استجابات أسعار الأسهم البطيئة

أخبار أرباح الشركات غير المتوقعة للأشهر اللاحقة ، وتفترض نظرية السوق الكفاء أن المعلومات العامة سوف يتم استيعابها في الأسعار بمجرد أن تصبح معروفة، الأمر الذي يتطلب من المستثمرين إعطاء الاهتمام الكامل لتسعير أصولهم. ومع ذلك، نظراً لأن الاهتمام محدود بسبب القيود المعرفية للمستثمرين فلا يستطيعون تتبع ومعالجة معلومات جميع الشركات المدرجة في السوق، لذلك يلعب اهتمام المستثمرين دوراً حيوياً في نشاط التداول الخاص بهم، مما يؤثر بالتالي على تسعير الأصول.

ولذلك، يتم دمج معلومات السوق في السعر بسرعة أكبر عندما تحظى الأسهم بمستوى أعلى من اهتمام المستثمرين، ومع ذلك فإن التحيزات السلوكية المختلفة تجعل نشاط تداول المستثمرين غير عقلاني، وخاصة بالنسبة للمستثمرين الأفراد، ومن ثم، فإن الاهتمام لا يشير إلى عقلانية التسعير، بل إن تطور المستثمر مهم أيضاً، فعندما يتخذ العديد من المستثمرين قرارات غير عقلانية بناءً على معتقدات ذاتية أو معلومات لا علاقة لها بأساسيات الشركة في السوق، فإن هناك صدمات مستمرة لأسعار الأسهم ، مما يؤدي إلى عدم توقع أسعار الأصول من خلال فرضية السوق الكفاء (Chen, et al., 2022). وبناء على ما سبق يمكن صياغة الفرض الإحصائي الأول على النحو التالي :

الفرض الأول: لا يوجد تأثير ذو دلالة إحصائية لمستويات الإفصاح الإجمالي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

٢/٣/٢ مقياس القابلية للقراءة وعلاقته باستجابة الأسهم لإعلان عن الأرباح

ترتبط سهولة قراءة إفصاحات الشركات بالسهولة التي يمكن بها للقارئ فهم النص المكتوب، فكلما كانت القوائم المالية أقل قابلية للقراءة، كلما زاد الوقت والجهد الذي يجب على المستخدمين تخصيصه لفك تشفير المعلومات ذات الصلة، مما يجعل تفسيرها أكثر صعوبة، إن صعوبة قراءة القوائم المالية تكون إما نتيجة لعدم قدرة

الإدارة على التواصل بوضوح أو أفعالها المتعمدة لتثويش المعلومات، كما استهدفت دراسة (Bonsall et al., 2017) معرفة إمكانية قراءة الإفصاح المالي بشأن نتائج سوق السندات، وتوصلت الدراسة إلى أن الإفصاحات المالية الأقل قابلية للقراءة تؤدي إلى انخفاض تصنيفات السندات وبالتالي ارتفاع تكلفة الديون، حيث إن الإفصاحات الأقل قابلية للقراءة تقلل من ثقة المستثمرين في المعلومات، مما يؤثر على الأحكام والقرارات المستقبلية.

وأفاد (Gao et al., 2020) في دراسته أن الإفصاحات أصبحت أكثر صعوبة في القراءة خلال فترة الدراسة، وأن عوامل مثل حجم الشركة ونسبة الأصول غير الملموسة في الميزانية العمومية والتغيرات في المديرين التنفيذيين ترتبط بسهولة القراءة، حيث أشارت الدراسة إلى أن الشركات الكبرى استخدمت في المتوسط، لغة أقل إثارة للجدل، لكن الشركات في الصناعات ذات الكثافة العالية لتكنولوجيا المعلومات التجارية (مثل خدمات المستهلك، والبرمجيات والخدمات، والخدمات المصرفية) استخدمت لغة أكثر إثارة للجدل من الشركات الأخرى.

وقارنت دراسة (Calderon & Gao., 2021) الإفصاحات عن مخاطر الأمن السيبراني للشركات الدولية والشركات الأمريكية، وأشارت الدراسة إلى أن الشركات الأجنبية تكشف المزيد عن مخاطر الأمن السيبراني الخاصة بها وأن إفصاحاتها أكثر قابلية للقراءة من الشركات الأمريكية، فسهولة قراءة الإفصاح يمكن أن تؤدي إلى خلاف بين المستثمرين من خلال اتجاهين :

يشير الاتجاه الأول إلى عدم تماثل المعلومات، فإذا اعتمد المستثمرون على مجموعات مختلفة من المعلومات عند صياغة آرائهم حول التدفقات النقدية المستقبلية، فمن المحتمل أن تتباين هذه الآراء، مما يؤدي إلى الخلاف. وعند الرد على إعلانات الأرباح، يقوم المستثمرون بدمج المعلومات الصادرة علناً مع معلومات الإعلان المسبق الخاصة بهم، سواء من الإفصاحات العامة أو المصادر الخاصة، كما أن انخفاض إمكانية قراءة الإفصاح النصي قد يسمح للمستثمرين المهرة فقط بفهم وضع

الشركة واستخلاص تقديرات أساسية صحيحة للتدفقات النقدية المستقبلية. وعلى العكس من ذلك فإن المستثمرين غير المحترفين لن يحصلوا على المعلومات أو يخطئوا في فهمها، سيؤدي هذا إلى خلاف بين المستثمرين غير المحترفين. بالإضافة إلى ذلك قد تصبح الإفصاحات غير القابلة للقراءة غير قادرة على التأثير على القرارات، مما يدفع المستثمرين إلى تجاهل الإفصاحات العامة والبحث عن معلومات خاصة بدلاً من ذلك.

أما الاتجاه الثاني فهو عدم التأكد بشأن تفسير أخبار الأرباح، يمكن أن يحدث هذا إذا كان على المستثمرين تقييم الخطأ والتحيز في الأرباح. على وجه الخصوص، يمكن للمستثمرين الحكم على انخفاض قابلية القراءة كعلامة على أن المديرين يحاولون التعتيم على الوضع لإخفاء النتائج السلبية (Lo et al., 2017) أو أن المديرين يجدون صعوبة في فهم بيئة الأعمال المضطربة بشكل خاص. سيؤدي هذا إلى شك المستثمرين في أن إشارة الأرباح تتأثر بالتحيز أو الخطأ. وبسبب الاختلافات في المهارات أو المعرفة أو السمات الفردية الأخرى، فمن المحتمل أن يختلف المستثمرون المختلفون حول حجم الخطأ، مما يؤدي إلى آراء متباينة حول تقييم الشركة.

ووفقاً لدراسة (Li et al., 2018) قد تقوم الإدارة بالتعتيم على البيانات المالية لإخفاء ضعف الأداء بسبب تعرضها لهجمات الأمن السيبراني، ويشير (Rjiba et al., 2021) إلى أن التقارير السنوية التي يصعب قراءتها تثني المستثمرين عن تقييم المعلومات، مما يقلل من نشاط تداول الأسهم، وفي هذه الحالة يظهر الغموض في الأرباح عندما يقدم إعلان الأرباح إشارة غير واضحة حول التدفقات النقدية المستقبلية، ويمكن أن تؤدي الإشارة الغامضة إلى مواجهة أسعار الأسهم للانخفاض لأن المستثمر يميل إلى التفاعل بشكل غير متكافئ مع الأخبار السلبية مقابل الأخبار الإيجابية، وإذا حدث هذا فمن غير المحتمل أن يتم التداول على المكشوف بعد صدور إشارة غامضة لأن أسعار الأسهم ستعكس السيناريو الأسوأ، والذي سيخفف من الأرباح المحتملة من البيع على المكشوف (المراجع: Rees & Twedt, 2021; ٢٠٢٢).

ووفقاً لما أشارت إليه دراسة (Tsafack, et al.,2023) يعد إعلان الأرباح بمثابة أمور أساسية في سوق الأوراق المالية، وتستجيب أسعار الأسهم بشكل إيجابي للإعلانات عن الأرباح التي تكون أكبر من المتوقع وسلباً للإعلانات عن الأرباح التي تكون أقل من المتوقع للشركات. كما توضح الدراسة ردود فعل كبيرة وسريعة لأسعار الأسهم على إعلانات الأرباح، وتشير إلى أن تقلبات الأسهم تزداد استجابةً لأخبار الأرباح، وأشارت الدراسة إلى أن الأسهم، في المتوسط، تحقق عوائد أعلى خلال الأشهر التي يتم فيها الإعلان عن الأرباح مقارنة بالأشهر التي لا يتم الإعلان فيها، كما تواجه الشركات في المتوسط زيادات في أسعار الأسهم خلال الفترات التي من المقرر أن تعلن فيها عن أرباحها.

وبناء على ما سبق ، يمكن صياغة الفرض الإحصائي الثاني على النحو التالي:

الفرض الثاني: لا يوجد تأثير ذو دلالة إحصائية لمستويات الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

٢/٣/٣ مقياس التقاضي وعلاقته باستجابة الأسهم للإعلان عن الأرباح

اعتبرت إحدى الدراسات التقاضي كمقياس لجودة الإفصاح العام عن مخاطر الأمن السيبراني، حيث ترتبط كلمات التقاضي، التي تعكس الميل إلى التنافس القانوني، بشكل كبير بالدعوى القضائية، وعند حدوث حوادث اختراق للأمن السيبراني يكون هناك زيادة كبيرة في استخدام لغة التقاضي (Gao et al., 2020) فعندما تفشل الشركات التي تواجه مخاطر أمنية سيبرانية عالية في تنبيه مستثمريها مسبقاً ثم تتعرض لحدث فعلي يتعلق بالأمن السيبراني، فقد تتعرض الشركات للدعوى القضائية. وبناء على ذلك، من المحتمل أن تكشف الإدارة عن مخاطر الأمن السيبراني، إذا كانت تعتقد بوجود احتمال كبير لحدوث خرق للأمن السيبراني في المستقبل (Li et al.,2018).

وفي هذا السياق أشارت دراسة (Tosun, 2021) إلى أن التأثير الكبير الذي تحدثه الإختراقات الأمنية على الشركات والجهات التنظيمية يمكن أن يكون مدمراً لسمعة الشركة، مما يؤدي إلى معدل دوران غير طبيعي للعملاء وفقدان السمعة ، الأمر الذي يؤثر بدوره على التدفقات النقدية والأرباح، إضافة إلى ذلك فإن حوادث الإختراقات الأمنية التي تكشف عن معلومات حساسة وسرية في التكوين لا يمكن أن تؤدي فقط إلى الدعاوى القضائية والعقوبات الحكومية، ولكن أيضاً إلى فقدان الميزة التنافسية ضد المنافسين في نفس الصناعة.

ترتبط دراسة (Tosun, 2021) بدراسة كلاً من (Corbet & Gurdgiev, 2020; Kamiya, et al, 2019) حول تأثير الجرائم الإلكترونية على تقلبات سوق الأسهم عبر الشركات المتداولة علناً، وتظهر هذه الدراسات أن الشركات المستهدفة تُعاقب بشكل كبير في شكل تقلبات سوق الأسهم، وعلى الرغم من أن دراسة (Corbet & Gurdgiev, 2019) تعتمد على الهجمات السيبرانية، فإنها تركز على أشكال أخرى من ردود أفعال السوق بخلاف التقلبات. كما تظهر دراسة (Kamiya et al, 2020) أن الهجمات السيبرانية من المحتمل أن تحدث في الشركات الأكبر حجماً والأكثر وضوحاً والأعلى قيمة، والشركات التي لديها أصول غير ملموسة أكثر، مع اهتمام أقل من مجلس الإدارة بإدارة المخاطر.

وتختلف دراسة (Tosun, 2021) عن دراسات (Corbet & Gurdgiev, 2020; Kamiya, et al, 2019) حيث تركز بشكل أكبر على رد فعل السوق الخالص للاختراقات الأمنية بدلاً من التركيز على العلاقة السببية العكسية بين خصائص الشركات والاختراقات الأمنية. وبعبارة أخرى، فإن الهدف هنا ليس تحديد العوامل التي تحرك نشاط القرصنة والحوافز الاقتصادية الأساسية، بل التحقيق في التأثير قصير وطويل الأجل على نشاط السوق وأساسيات الشركات. على الرغم من النمو السريع، إلا أن الأدبيات المتعلقة بالتكاليف المالية للانتهاكات الأمنية ضعيفة إلى حد ما.

كما أشارت دراسة (Florackis, et al., 2023) إلى أن الإفصاحات الاختيارية المتعلقة بأمن المعلومات قد تخفف من تكاليف التقاضي المحتملة وتخفض تكلفة رأس مال الشركة عن طريق تقليل عدم تماثل المعلومات بين إدارة الشركة ومستثمريها، وهذا يدل على وجود ارتباط إيجابي بين الإفصاح الاختياري وقيمة الشركة، كما أن هامش العرض والطلب للشركات التي تقدم إفصاحات اختيارية عن أمن المعلومات أقل إحصائياً من الشركات التي لا تقدم مثل هذا الإفصاح، وتشير الأدلة التجريبية للأدبيات السابقة (Kamiya et al., 2020) إلى أن الاختراقات الأمنية تمثل صدمة سلبية مكلفة لسمعة الشركات المتداولة علناً، وبالتالي تؤثر سلباً على توقعات المستثمرين بشأن التدفقات النقدية المستقبلية للشركات المستهدفة، ويعرضها لمخاطر التقاضي.

توفر دراسة (Tosun, 2021) دليلاً قوياً على رد فعل السوق تجاه الهجمات السيبرانية، خاصة على المدى القصير، حيث تظهر الشركات المتضررة من الاختراقات الأمنية أداء سيء بشكل كبير، ويكون ذلك مشروطاً بعدة متغيرات أساسية، مثل حجم الشركة والرافعة المالية والممتلكات النقدية ومقاييس الربحية والاستثمارات. وترتبط إعلانات الاختراقات الأمنية سلباً بتغيرات أسعار الأسهم خلال يومين من تاريخ الإعلان، فقد يكون للإعلان عن اختراق أمني للشركة تأثير سلبي يبلغ حوالي 1% من القيمة السوقية للشركة في الأيام التالية للحدث، وفي الواقع فإن الغالبية العظمى من اختراقات البيانات لا تؤثر بشكل مباشر على المنتجات أو الخدمات إنما تؤثر على سمعة الشركة وتعرضها بشكل كبير لمخاطر التقاضي.

وبناء على ما سبق يمكن عرض الفرض الإحصائي الثالث على النحو التالي:

الفرض الثالث: لا يوجد تأثير ذو دلالة إحصائية لمستويات الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

٣. الدراسة التطبيقية

تعتمد منهجية البحث على استخدام تحليل المحتوى للتقارير الملحقة بالقوائم المالية للبنوك المدرجة في سوق الأوراق المالية المصري.

٣/١ مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في كافة البنوك المقيدة في سوق الأوراق المالية المصري والتي يبلغ عددها ١٢ بنك ، وفي إطار بدء اهتمام تلك البنوك بالإفصاح عن مخاطر الأمن السيبراني خلال فترة ما قبل وباء الكورونا بناء على توجيهات البنك المركزي المصري نتيجة وجود المزيد من الهجمات السيبرانية المختلفة على عدد من البنوك المصرية، بدأ استخدام تقارير الحوكمة كوسيلة للإفصاح عن مخاطر الأمن السيبراني بشكل عام تحت مسمى مخاطر أمن المعلومات في تلك التقارير والإفصاح عنها بشكل نصي.

وتأسيساً على ذلك، يبلغ عدد البنوك المقيدة في سوق الأوراق المالية المصري خلال هذه الفترة عدد ١٢ بنك تقريباً، ونظراً لأن تقارير الحوكمة بدأت تهتم بمخاطر الأمن المعلوماتي بدءاً من عام ٢٠١٨ في أعقاب الهجمات السيبرانية المختلفة وتزايد هذا الاهتمام أكثر في عام ٢٠٢٠ نتيجة وجود وباء الكورونا على مستوى العالم، فإنه يمكن القول أن عينة الدراسة تبدأ من عام ٢٠١٨ حتى عام ٢٠٢٢ بما يسجل ٦٠ مشاهدة خلال الفترة الزمنية (١٢ بنك × ٥ سنوات). ويمكن توضيح البنوك المدرجة بعينة الدراسة من خلال الجدول التالي:

جدول رقم (١): أسماء البنوك المدرجة بعينة الدراسة

م	اسم البنك
١	البنك التجاري الدولي
٢	البنك المصري الخليجي
٣	البنك المصري لتنمية الصادرات

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

بنك البركة مصر	٤
بنك التعمير والاسكان	٥
بنك الشركة المصرفية العربية الدولية	٦
بنك القاهرة	٧
بنك فيصل الاسلامي	٨
بنك قطر الوطني الأهلي	٩
بنك قناة السويس	١٠
بنك كريدي أجريكول مصر	١١
مصرف أبوظبي الاسلامي	١٢

٣/٢ متغيرات الدراسة وأدوات القياس:

انطلاقاً من العرض السابق للدراسة النظرية والفروض الإحصائية المراد اختبارها يمكن صياغة أدوات قياس الدراسة من خلال العرض التالي:

٣/٢/١ الإفصاح عن مخاطر الأمن السيبراني:

يتبين أن موضوعات الإفصاح عن مخاطر الأمن السيبراني وهي المتغير المستقل للدراسة تتركز في ثلاثة مواضع أساسية تتمثل في: الموضوعات الدالة على مخاطر الأمن السيبراني بتقارير الحوكمة، وقابلية الإفصاح عن مخاطر الأمن السيبراني للقراءة، وأخيراً استخدام لغة التقاضي عن مخاطر الأمن السيبراني بتقارير الحوكمة بالبنوك. وفي هذا الشأن، يمكن تقسيم الإفصاح عن مخاطر الأمن السيبراني وفقاً لثلاثة أقسام على النحو الوارد بالجدول رقم (٢) :

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

جدول رقم (٢)

مقاييس جودة الإفصاح عن مخاطر الأمن السيبراني	
القسم الأول: مؤشر الإفصاح العام عن مخاطر الأمن السيبراني: المكونات	
أولاً: معلومات الأمن السيبراني : إدارة متخصصة	مكونات مؤشر الإفصاح العام
١- وجود فريق لإدارة المخاطر الإلكترونية متعدد الوظائف مع تحديد واضح لأهداف الشركة المتعلقة بإدارة مخاطر الأمن السيبراني.	
٢- دمج الشركة إدارة المخاطر السيبرانية في الخطة الاستراتيجية .	
٣- إدارة المخاطر السيبرانية التي تواجهها الشركة والتي تؤثر على تحقيقها لأهدافها ، واتخاذ القرارات بشأن الرقابة عليها.	
ثانياً: تصميم وصيانة هيكل رقابي لمعلومات أمن السيبراني	
٤- مواجهه المخاطر وعمل تقييم مستمر للتأكد من فاعلية تصميم وتشغيل الضوابط الداخلية ، ومعالجة أوجه القصور واتخاذ الإجراءات التصحيحية .	
٥- التقرير عن الأنشطة والسياسات والإجراءات الرسمية للرقابة على التكنولوجيا	
٦- تحديد وتحليل وتقييم المخاطر السيبرانية التي تواجه الشركة مع منع أو اكتشاف المخاطر السيبرانية.	
٧- تقييم المخاطر بطريقة شاملة ، متضمنة مدى كفاية الإجراءات الوقائية المتخذة.	
٨- ضمان المخاطر السيبرانية عند مستوى مقبول.	
٩- تقليل مخاطر الأمن السيبراني ، والاخذ في الاعتبار مخاطر الصناعة ، الاعتبارات البيئية والتكنولوجية ، التغيرات التنظيمية والتغيرات الأخرى بالإضافة الي تحديد التكاليف والعواقب المحتملة والناجمة عن هذه الحوادث.	
ثالثاً: دعم هيكل الرقابة الداخلية	
١٠- دعم هيكل الرقابة الداخلية بالمزيد من المعلومات الخارجية ذات الصلة التجارية والصناعية.	
١١- نشر أنشطة الرقابة في شكل مجموعة من السياسات والإجراءات .	
رابعاً: الالتزام بالإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية	
١٢- تحديد أنواع ومدى تكرار حدوثها على مدار السنة.	
١٣- الإفصاح الدوري عن الاستراتيجيات والسياسيات والإجراءات المتبعة في حوكمة مخاطر الأمن السيبراني، تحديد المسؤول عن حوكمة الأمن السيبراني .	
١٤- الالتزام بالتقرير عن النزاهة والأخلاق وفقاً لمعايير السلوك بالشركة ، تحديد ومعالجة الانحرافات لدعم أداء برنامج مخاطر الأمن السيبراني .	

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

القسم الثاني: الإفصاح عن مخاطر الأمن السيبراني: القابلية للقراءة	
وفقاً لدراسة (Calderon & Gao, 2021) يمكن الاعتماد على مؤشر FOG لتحليل المحتوى المتعلق بالقابلية للقراءة لمحتوى الإفصاح المحاسبي بشكل عام مع تخصيصه للغة الإفصاح عن مخاطر الأمن السيبراني، ومن ثم يمكن للدراسة الحالية استخدام مؤشر افصاح FOG في الدراسة الحالية وفقاً للمعادلة التالية: القابلية للقراءة = $0.4 \times (\text{عدد الكلمات بالجملة فيما يتعلق بالأمن السيبراني} + \text{نسبة الكلمات المعقدة فيما يتعلق بالأمن السيبراني})$.	مؤشر FOG لتحليل المحتوى المتعلق بالقابلية للقراءة لمحتوى الإفصاح المحاسبي
القسم الثالث: الإفصاح عن مخاطر الأمن السيبراني: لغة التقاضي	
ويمكن للدراسة الاعتماد على منهج حقبة الكلمات الدالة على التقاضي bag-of-words approach باستخدام أسلوب تحليل المحتوى أيضاً وفقاً لدراسة (Calderon & Gao, 2021) ، ومن ثم يمكن الاعتماد على متغيرات لغة التقاضي كمؤشر للإفصاح عن لغة التقاضي باستخدام المعادلة التالية: لغة التقاضي = عدد كلمات التقاضي فيما يتعلق بالأمن السيبراني ÷ إجمالي عدد الكلمات المتعلقة بالأمن السيبراني.	نهج حقبة الكلمات الدالة على التقاضي bag-of-words approach باستخدام أسلوب تحليل المحتوى أيضاً

٣/٢/٢ استجابة أسعار الأسهم للإعلان عن الأرباح:

يعبر المتغير التابع للدراسة عن استجابة أسعار الأسهم للإعلان عن الأرباح، وفي هذا الشأن يمكن تلخيص أدوات قياس استجابة أسعار الأسهم للإعلان عن الأرباح وفقاً للجدول التالي اتباعاً لدراسة (Blankespoor, et al., 2019):

جدول رقم (٣): مقاييس استجابة أسعار الأسهم للإعلان عن الأرباح

المتغير	الرمز	طريقة القياس
معدل دوران العوائد غير العادية للمستثمر بعد اعلان الأرباح	Abn_IndivVol	المتوسط اليومي لنسبة تداول الأسهم من المستثمرين خلال أيام من ٢٠- بعد اعلان الأرباح مطروحة من المتوسط خلال الفترة قبل الاعلان - ١١ إلى -٤١ يوم قبل الاعلان مقسومة على ١٠٠
معدل دوران العوائد غير العادية للمستثمر بالأسهم المشتراة بعد اعلان الأرباح	Abn_BuyVol	المتوسط اليومي لنسبة الأسهم المشتراة من المستثمرين خلال أيام من ٢٠- بعد اعلان الأرباح مطروحة من المتوسط خلال الفترة قبل الاعلان - ١١ إلى -٤١ يوم قبل الاعلان مقسومة على ١٠٠

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

<p>المتوسط اليومي لنسبة الأسهم المباعة من المستثمرين خلال أيام من ٢٠٠ بعد اعلان الأرباح مطروحة من المتوسط خلال الفترة قبل الاعلان - ١١ إلى ٤١ يوم قبل الاعلان مقسومة على ١٠٠</p>	<p>Abn_SellVol</p>	<p>معدل دوران العوائد غير العادية للمستثمر بالأسهم المباعة بعد اعلان الأرباح</p>
$VOL_R = \frac{1}{D} + \sum_{d=1}^{Dt} (R_i + MR_i)$ <p>حيث أن:</p> <p>$VOL_R =$ تشير إلى مستوى التقلب في عوائد الأسهم؛</p> <p>$D =$ عدد أيام التداول بعد اعلان الأرباح؛</p> <p>$R_i =$ عائد السهم اليومي في اليوم d والشركة i؛</p> <p>$MR_i =$ متوسط العائد اليومي للسهم i خلال الفترة الخاصة بالتداول بعد اعلان الأرباح.</p>	<p>VOL_R</p>	<p>التقلب في عوائد الأسهم الإجمالي بعد اعلان الأرباح</p>

٣/٢/٣ المتغيرات الضابطة:

ويمكن في هذا الصدد تحديد أثر المتغير المستقل على المتغير التابع للدراسة من خلال ادراج بعض المتغيرات الضابطة لنموذج اختبار الفروض الإحصائية للدراسة اتباعاً للعديد من الدراسات السابقة ذات الصلة، والتي يمكن تلخيصها وفقاً للجدول التالي:

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...
د/ أحمد محمد علي أبو سمك

جدول رقم (٤): المتغيرات الرقابية

المتغير	الرمز	التفسير
نسبة القيمة السوقية الى الدفترية	BTM	إجمالي قيمة الشركة السوقية مقسومة على إجمالي القيمة الدفترية؛
حجم الشركة	SIZE	لوغاريتم إجمالي أصول الشركة؛
نسبة الملكية المؤسسية	Inst_Own	نسبة الأسهم المملوكة لكبار المستثمرين المؤسسيين إلى إجمالي عدد الأسهم؛
مؤشر الخسارة	LOSS	متغير وهمي، بحيث يأخذ القيمة 1 في حالة وجود خسارة، بينما يأخذ القيمة صفر فيما عدا ذلك.

٣/٣ الإحصاء الوصفي:

يمكن للباحث تلخيص الإحصاءات الوصفية لعينة الدراسة وفقاً للجدول التالي:

جدول رقم (٥): نتائج الإحصاءات الوصفية

Variables	N	Mean	Std. Dev.	Skewness	Kurtosis	Min.	Max.
Abn_IndivVol	60	0.36	0.89	0.78	2.48	-0.06	0.48
Abn_BuyVol	60	0.23	0.57	0.81	2.47	0.15	0.26
Abn_SellVol	60	0.21	0.48	0.62	2.79	0.12	0.27
VOL_R	60	0.41	0.57	0.73	2.10	0.08	0.68
CC_M	60	1.75	0.55	0.73	1.93	1.00	4.00

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

CC_CS	60	3.21	0.62	0.94	1.61	1.00	8.00
CC_IC	60	1.00	0.11	0.94	2.84	1.00	2.00
CC_CA	60	1.26	0.57	0.94	2.52	1.00	3.00
TCC	60	6.53	0.91	0.84	1.74	1.00	17.00
Read	60	31.80	7.50	0.55	2.76	26.80	37.25
Litigious	60	0.03	0.01	0.55	1.65	0.00	0.04
BTM	60	0.68	0.51	0.75	2.58	0.33	0.73
SIZE	60	5.25	1.15	0.88	2.00	3.24	9.32
Inst_Own	60	0.33	0.25	0.73	2.97	0.00	0.42
LOSS	60	0.28	0.11	0.96	2.21	0.00	1.00

يتبين من خلال العرض السابق للإحصاءات الوصفية مجموعة من الملاحظات التي يمكن بيانها فيما يلي:

يتضح أن المتوسط الحسابي للمتغيرات الخاصة بالإفصاح العام عن مخاطر الأمن السيبراني المتمثلة في CC_M, CC_CS, CC_CI, CC_CA تبلغ ١,٧٥، ٣,٢١، ١، ١,٢٦، ٦,٥٣، وهو ما يشير إلى أن توافر عناصر الإفصاح عن الأمن السيبراني بشكل نسبي في تقارير الحوكمة التي تقدمها البنوك المدرجة في سوق الأوراق المالية المصري، وبالنسبة للمتغيرات المتعلقة باستجابات أسعار الأسهم عقب اعلان الأرباح يتبين للباحث أن المتغيرات Abn_IndivVol, Abn_BuyVol, Abn_SellVol, VOL_R يتبين أن أوساطها الحسابية تبلغ ٠,٣٦، ٠,٢٣، ٠,٢١، ٠,٤١ على التوالي وهو ما يشير إلى اعتدالية المتوسطات الحسابية لتلك المتغيرات بين الحدود الدنيا والقصى للعينة.

كما يتضح ارتفاع المتوسط الحسابي للمتغير Read الخاص بقابلية الإفصاح السيبراني للقراءة حيث يبلغ ٣١,٨٠ هو ما يقترب إلى حد كبير من الحد الأقصى للعينة وهو ما يشير إلى ارتفاع هذا المؤشر بعينة الدراسة إلى حد كبير، وانخفاض المتوسط الحسابي للمتغير Litigious الخاص بلغة التقاضي حيث أنه يبلغ ٠,٠٣ ، وتشير تلك النتائج إلى أن لغة التقاضي المتعلقة بالأمن السيبراني بشكل عام منخفضة إلى حد كبير في البيئة المصرية.

٣/٤ مصفوفة ارتباط بيرسون:

ويتضح من معاملات الارتباط المدرجة بالجدول وجود علاقة طردية معنوية بين مستويات الإفصاح عن الأمن السيبراني بأقسامه الثلاثة سواء كان الإفصاح العام أو القابلية للقراءة أو لغة التقاضي، ومؤشرات استجابة أسعار الأسهم للإعلان عن الأرباح حيث أن زيادة مستوى الإفصاح المحاسبي عن مخاطر الأمن السيبراني يحدث ارتفاع في مستوى تقلبات العوائد غير العادية للأسهم عقب إعلانات الأرباح، وهو ما يعطي دلالة للمستثمر على وجود شفافية في التعاملات الاستثمارية الخاصة بالشركة وإضافة إلى ذلك توضح النتائج أهمية الإفصاح عن مخاطر الأمن السيبراني لدى المستثمر.

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

جدول رقم (٦): مصفوفة ارتباط بيرسون

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1 Abn_IndivVol	1														
2 Abn_BuyVol	0.22*	1													
3 Abn_SellVol	0.41*	0.29*	1												
4 VOL_R	0.31*	0.40*	0.34*	1											
5 CC_M	0.23*	0.37*	0.22*	0.40*	1										
6 CC_CS	0.41*	0.40*	0.36*	0.33*	0.33*	1									
7 CC_IC	0.23*	0.39*	0.32*	0.23	0.23*	0.22*	1								
8 CC_CA	0.39*	0.22*	0.23*	0.35*	0.41*	0.41*	0.32*	1							
9 TCC	0.35*	0.21*	0.23*	0.22*	0.36*	0.37*	0.24*	0.38*	1						
10 Read	0.41*	0.38*	0.26*	0.40*	0.24*	0.39*	0.26*	0.34*	0.35*	1					
11 Litigious	0.31*	0.26*	0.26*	0.40*	0.33*	0.32*	0.23*	0.33*	0.34*	0.39*	1				
12 BTM	0.04	0.03	0.03	0.05	0.03	0.02	0.05	0.02	0.05	0.05	0.04	1			
13 SIZE	0.02	0.01	0.01	0.03	0.05	0.05	0.04	0.04	0.03	0.02	0.02	0.03	1		
14 Inst_Own	0.02	0.05	0.02	0.05	0.05	0.02	0.03	0.02	0.04	0.02	0.05	0.02	0.02	1	
15 LOSS	0.01	0.03	0.02	0.04	0.02	0.02	0.04	0.06	0.02	0.05	0.01	0.02	0.01	0.04	1

* تشير إلى معنوية تلك المعاملات عند مستوى ٥%.

كما يتضح أن قيم معاملات الارتباط بين المتغيرات المستقلة أقل من ٠,٨ وهو ما يشير إلى عدم وجود أي مشكلة من مشاكل الأزواج الخطي بين المتغيرات وهو ما يشير إلى صحة نماذج اختبار الفروض الإحصائية للدراسة بشكل مبدئي (Hair et al,2014).

٣/٥ نتائج اختبارات الفروض الإحصائية للدراسة:

يهدف هذا الجزء من الدراسة إلى تحليل آثار الإفصاح عن مخاطر الأمن السيبراني بأقسامه الثلاثة على استجابة أسعار الأسهم عقب إعلانات الأرباح، والتي تتمثل في: أثر الإفصاح الإجمالي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح، وأثر الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح، وأثر الإفصاح باستخدام لغة التقاضي عن

مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح. ويمكن توضيح نتائج اختبار الفروض الإحصائية للدراسة على النحو التالي:

٣/٥/١ نتيجة اختبار الفرض الإحصائي الأول للدراسة:

يتنبأ الفرض الأول بتحليل أثر الإفصاح الإجمالي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم لإعلان الأرباح، ومن ثم يمكن صياغة نموذج اختبار الفرض الإحصائي الأول للدراسة على النحو التالي:

$$\text{Abn_IndivVol} = \beta_0 + \beta_1(\text{CC_M}) + \beta_2(\text{CC_CS}) + \beta_3(\text{CC_IC}) + \beta_4(\text{CC_CA}) + \beta_5(\text{TCC}) + \beta_6(\text{BTM}) + \beta_7(\text{SIZE}) + \beta_8(\text{Inst_Own}) + \beta_9(\text{LOSS}) + \varepsilon \quad (1-1)$$

$$\text{Abn_BuyVol} = \beta_0 + \beta_1(\text{CC_M}) + \beta_2(\text{CC_CS}) + \beta_3(\text{CC_IC}) + \beta_4(\text{CC_CA}) + \beta_5(\text{TCC}) + \beta_6(\text{BTM}) + \beta_7(\text{SIZE}) + \beta_8(\text{Inst_Own}) + \beta_9(\text{LOSS}) + \varepsilon \quad (1-2)$$

$$\text{Abn_SellVol} = \beta_0 + \beta_1(\text{CC_M}) + \beta_2(\text{CC_CS}) + \beta_3(\text{CC_IC}) + \beta_4(\text{CC_CA}) + \beta_5(\text{TCC}) + \beta_6(\text{BTM}) + \beta_7(\text{SIZE}) + \beta_8(\text{Inst_Own}) + \beta_9(\text{LOSS}) + \varepsilon \quad (1-3)$$

$$\text{VOL_R} = \beta_0 + \beta_1(\text{CC_M}) + \beta_2(\text{CC_CS}) + \beta_3(\text{CC_IC}) + \beta_4(\text{CC_CA}) + \beta_5(\text{TCC}) + \beta_6(\text{BTM}) + \beta_7(\text{SIZE}) + \beta_8(\text{Inst_Own}) + \beta_9(\text{LOSS}) + \varepsilon \quad (1-4)$$

حيث أن:

CC_M = قيمة الإفصاح عن إنشاء إدارة خاصة بالأمن السيبراني؛ CC_CS = قيمة الإفصاح عن تصميم هيكل رقابة للأمن السيبراني؛ CC_IC = قيمة الإفصاح عن دعم هيكل الرقابة الداخلية للأمن السيبراني؛ CC_CA = قيمة الإفصاح عن الالتزام بالإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية؛ TCC = إجمالي قيمة الإفصاح عن الأمن السيبراني.

لتحليل العلاقة بين متغيرات الفرض الأول تم بتشغيل نموذج اختبار الفروض رقم (١) واعتماداً على تحديد طبيعة العلاقة من خلال مستوى معنوية العلاقة واتجاهات وقيم معاملات المتغيرات المدرجة بنموذج اختبار الفروض رقم (١) تم التوصل إلى النتائج المعروضة بالجدول رقم (٧).

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

ويتضح من خلال النتائج المعروضة بالجدول رقم (٧) الارتفاع النسبي بالقوة التفسيرية للنموذج حيث تبلغ $36,8\%$ ، $39,2\%$ ، $38,8\%$ ، $36,9\%$ على التوالي، وهو ما يشير إلى أن المتغيرات المستقلة والحاكمة الموجودة بنموذج اختبار الفروض الإحصائية رقم (١) للدراسة يمكنها تفسير التباين الكلي في استجابة أسعار الأسهم لإعلانات الأرباح باستخدام التقلب في التداول، والتقلب في البيع، والتقلب في الشراء، والتقلب العام في الأسعار بنسبة $36,8\%$ ، $39,2\%$ ، $38,8\%$ ، $36,9\%$ ، وهي نتيجة جيدة تقترب من نظيرتها بالعديد من الدراسات ذات الصلة. وبالتالي، فإن نموذج اختبار الفروض رقم (٧) يمكنه تفسير العلاقة بكفاءة بين المتغيرات الداخلة فيه.

جدول رقم (٧): نتيجة اختبار الفرض الإحصائي الأول للدراسة

	Panel (A): Abn_IndivVol		Panel (B): Abn_BuyVol		Panel (C): Abn_SellVol		Panel (D): VOL_R	
	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.
Constant	0.079	0.698	0.041	0.953	0.052	0.761	0.086	0.549
CC_M	0.381	4.019***	0.385	2.536***	0.222	4.011***	0.299	2.573***
CC_CS	0.289	3.266***	0.297	4.013***	0.229	3.393***	0.265	2.291***
CC_IC	0.332	3.036***	0.248	3.968***	0.388	3.347***	0.330	3.033***
CC_CA	0.411	3.265***	0.325	3.144***	0.345	2.462***	0.449	3.253***
TCC	0.348	3.888***	0.242	2.759***	0.348	3.001***	0.278	3.290***
BTM	0.020	0.995	0.025	0.999	0.070	0.559	0.062	0.839
SIZE	0.063	0.709	0.083	0.728	0.060	0.569	0.040	0.761
Inst_Own	0.086	0.703	0.057	0.666	0.078	0.716	0.087	0.678
LOSS	0.048	1.012	0.064	0.946	0.086	0.952	0.049	0.642
Obs.	60		60		60		60	
R2	0.368		0.392		0.388		0.369	
Adj R2	0.355		0.381		0.372		0.358	
Std. Error	0.441		0.391		0.325		0.318	
F Value	327.415		369.247		324.258		316.247	
	(P = 0.000)		(P = 0.000)		(P = 0.000)		(P = 0.000)	

*** تشير إلى مستوى معنوية ٥%

وتشير نتائج العمود الأول (Panel A) إلى معنوية المتغيرات المستقلة TCC، CC_CA، CC_IC، CC_CS، CC_M المتعلقة بإنشاء إدارة خاصة بالأمن السيبراني، وتصميم هيكل رقابة للأمن السيبراني، ودعم هيكل الرقابة الداخلية، والالتزام بالإفصاح عن المعلومات المتعلقة بالحوادث السيبرانية، وإجمالي الإفصاح عن الأمن السيبراني حيث أن (t-stat. = 4.019, 3.266, 3.036,

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد على أبو سمك

(2) $3.888 > 3.265$ كما تشير نتائج (Panel B) إلى أن (t-stat. = 2.536)
(2) $3.144, 2.759 > 3.968, 4.013$ ، بالإضافة إلى ذلك، تشير نتائج (Panel
C) إلى أن (t-stat. = 4.011, 3.393, 3.347, 2.462, 3.001 > 2) ، وتشير
نتائج (Panel D) إلى أن (t-stat. = 2.573, 2.291, 3.033, 3.253, 3.290 > 2)
كما أنها جميعاً تحمل إشارة موجبة.

وهو ما يشير إلى أن ارتفاع مستوى الإفصاح عن الأمن السيبراني بكافة أشكاله يؤدي إلى زيادة التقلب في استجابة أسعار الأسهم عن إعلانات الأرباح باستخدام التداول العام، التقلب في الشراء، التقلب في البيع، التقلب العام في الأسعار، حيث تزداد مستوى التقلبات في العوائد غير العادية للسهم عقب إعلانات الأرباح، وهو ما يتفق مع دراسة (Truong, 2023) على أن إعلانات الأرباح تعد مصدراً مهماً للمعلومات وللتقييم الأساسي للشركات، فالتحركات الكبيرة في أسعار الأسهم حول إعلانات الأرباح تدل على أن الشركات ذات نتائج الأرباح الإيجابية (السلبية) تواجه أداءً إيجابياً (سلبياً) غير طبيعي في أسعار الأسهم، حيث توفر إعلانات الأرباح بيئة جذابة لدراسة تأثيرات الأدلة في توقيت الإفصاح. وهو ما يؤكد أن الإفصاح السيبراني له قدرة كبيرة في التأثير على وعي المستثمر المستخدم الخارجي للقوائم المالية كما أنه يحفز قراراته الاستثمارية وحجم التداول في سوق الأوراق المالية المصري للبنوك المدرجة.

وأخيراً يتبين عدم معنوية أي متغير من المتغيرات الضابطة، ومن ثم فلن يكون لأي منهما تأثير على المتغير التابع الخاص باستجابة أسعار الأسهم عقب إعلانات الأرباح باستخدام التقلب في (التداول، الشراء ، البيع، التقلب العام في الأسعار)، وبناء على النتائج السابق عرضها يمكن قبول الفرض الإحصائي الأول للدراسة على الشكل البديل التالي: يوجد تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح العام عن الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

٣/٥/٢ نتيجة اختبار الفرض الإحصائي الثاني للدراسة:

يتنبأ الفرض الثاني بتحليل أثر الإفصاح باستخدام قابلية القراءة عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم لإعلان الأرباح، ومن ثم يمكن صياغة نموذج اختبار الفرض الإحصائي الثاني للدراسة على النحو التالي:

$$\text{Abn_IndivVol} = \beta_0 + \beta_1(\text{Read}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (2-1)$$

$$\text{Abn_BuyVol} = \beta_0 + \beta_1(\text{Read}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (2-2)$$

$$\text{Abn_SellVol} = \beta_0 + \beta_1(\text{Read}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (2-3)$$

$$\text{VOL_R} = \beta_0 + \beta_1(\text{Read}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (2-4)$$

حيث أن:

Read = قيمة مؤشر القابلية للقراءة السابق عرضه بالجدول رقم (٢)

ولتحليل العلاقة بين متغيرات الفرض الثاني تم بتشغيل نموذج اختبار الفروض رقم (٢) واعتماداً على تحديد طبيعة العلاقة من خلال مستوى معنوية العلاقة واتجاهات وقيم معاملات المتغيرات المدرجة بنموذج اختبار الفروض رقم (٢) تم التوصل إلى النتائج المعروضة بالجدول رقم (٨).

ويتضح لدى الباحث من خلال النتائج المعروضة بالجدول رقم (٨) الارتفاع النسبي بالقوة التفسيرية للنموذج حيث تبلغ ٤١,١%، ٣٩,٨%، ٣٨,٦%، ٣٩,٥% على التوالي، وهو ما يشير إلى أن المتغيرات المستقلة والحاكمة الموجودة بنموذج اختبار الفروض الإحصائية رقم (٢) للدراسة يمكنها تفسير التباين الكلي في استجابة أسعار الأسهم لإعلانات الأرباح باستخدام النقلب في التداول، والنقلب في البيع، والنقلب في الشراء، والنقلب العام في الأسعار بنسبة ٤١,١%، ٣٩,٨%، ٣٨,٦%، ٣٩,٥% وهي نتيجة

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

جيدة تقترب من نظيرتها بالعديد من الدراسات ذات الصلة. وبالتالي، فإن نموذج اختبار الفروض رقم (٢) يمكنه تفسير العلاقة بكفاءة بين المتغيرات الداخلة فيه.

جدول رقم (٨): نتيجة اختبار الفرض الإحصائي الثاني للدراسة

	Panel (A): Abn_IndivVol		Panel (B): Abn_BuyVol		Panel (C): Abn_SellVol		Panel (D): VOL_R	
	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.
Constant	0.059	0.549	0.053	1.073	0.039	0.901	0.082	0.783
Read	0.266	3.167***	0.276	2.929***	0.448	2.374***	0.392	2.691***
BTM	0.088	0.591	0.038	0.948	0.084	0.623	0.089	0.979
SIZE	0.019	0.595	0.072	0.640	0.056	1.046	0.066	0.885
Inst_Own	0.048	0.716	0.058	0.923	0.045	1.023	0.047	0.752
LOSS	0.061	1.049	0.072	0.903	0.095	1.057	0.048	0.731
Obs.	60		60		60		60	
R2	0.411		0.398		0.386		0.395	
Adj R2	0.397		0.383		0.377		0.361	
Std. Error	0.446		0.444		0.432		0.419	
F Value	326.588		329.365		368.147		349.581	
	(P = 0.000)		(P = 0.000)		(P = 0.000)		(P = 0.000)	

*** تشير إلى مستوى معنوية ٥%

وتشير نتائج (Panel A) إلى معنوية المتغير المستقل Read الخاص بالإفصاح عن مخاطر الأمن السيبراني باستخدام القابلية للقراءة حيث أن (t-stat. = 3.167 > 2) ، كما تشير (Panel B) إلى أن (t-stat. = 2.929 > 2) كما تشير نتائج (Panel C) إلى أن (t-stat. = 2.374 > 2) ، كما تشير نتائج (Panel D) إلى أن (t-stat. = 2.691 > 2) ، وجميعها تحمل إشارة موجبة وهو ما يشير إلى أن ارتفاع مستوى الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني يؤدي إلى زيادة التقلب في استجابة أسعار الأسهم عن إعلانات الأرباح باستخدام التداول العام، التقلب في الشراء والتقلب في البيع ومستويات التقلبات العامة حيث تزداد مستوى التقلبات في العوائد غير العادية للسهم عقب إعلانات الأرباح ، وهو ما يؤكد على تأثير الإفصاح السيبراني باستخدام القابلية للقراءة بقدرة كبيرة على وعي

المستثمر قدرته على قراءة للقوائم المالية كما أنه يحفز قراراته الاستثمارية وحجم التداول في سوق الأوراق المالية المصري للبنوك المدرجة. وتتفق الدراسة الحالية مع دراسة (Truong, 2023) في أنه يمكن للبنوك التنافس من خلال اختيار موعد الإعلان عن الأرباح، فمن خلال الإعلان في وقت مبكر عن نظيراتها، يمكن للشركة جذب انتباه السوق بعيداً عن الشركات الأخرى، حيث تولد الخسارة المحتملة لاهتمام السوق قوة تنافسية تحفز الشركات الأخرى على الاستجابة والإعلان مبكراً أيضاً لمواجهة أي اهتمام مفقود من المستثمرين. وأخيراً يتبين عدم معنوية أي متغير من المتغيرات الضابطة، ومن ثم فلن يكون لأي منهما تأثير على المتغير التابع الخاص باستجابة أسعار الأسهم عقب إعلانات الأرباح باستخدام التقلب في الشراء، التقلب في البيع، التقلب العام في الأسعار، وبناء على النتائج السابق عرضها يمكن قبول الفرض الإحصائي الثاني للدراسة على الشكل البديل التالي: يوجد تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

٣/٥/٣ نتيجة اختبار الفرض الإحصائي الثالث للدراسة:

يتنبأ الفرض الثالث بتحليل أثر الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم لإعلان الأرباح، ومن ثم يمكن للباحث صياغة نموذج اختبار الفرض الإحصائي الثالث للدراسة على النحو التالي:

$$\text{Abn_IndivVol} = \beta_0 + \beta_1(\text{Litigious}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (3-1)$$

$$\text{Abn_BuyVol} = \beta_0 + \beta_1(\text{Litigious}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (3-2)$$

$$\text{Abn_SellVol} = \beta_0 + \beta_1(\text{Litigious}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (3-3)$$

$$\text{VOL_R} = \beta_0 + \beta_1(\text{Litigious}) + \beta_2(\text{BTM}) + \beta_3(\text{SIZE}) + \beta_4(\text{Inst_Own}) + \beta_5(\text{LOSS}) + \varepsilon \quad (3-4)$$

قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة ...

د/ أحمد محمد علي أبو سمك

جدول رقم (٩): نتيجة اختبار الفرض الإحصائي الثالث للدراسة

	Panel (A): Abn_IndivVol		Panel (B): Abn_BuyVol		Panel (C): Abn_SellVol		Panel (D): VOL_R	
	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.	OLS Estimate	t-stat.
Constant	0.073	0.946	0.061	0.814	0.055	0.604	0.064	0.939
Litigious	0.318	3.978***	0.226	2.649***	0.436	3.074***	0.354	3.328***
BTM	0.019	1.052	0.077	0.590	0.044	0.567	0.051	0.883
SIZE	0.092	1.072	0.094	1.040	0.041	0.904	0.073	0.858
Inst_Own	0.022	0.594	0.036	0.748	0.060	0.883	0.022	0.745
LOSS	0.040	0.763	0.092	1.112	0.045	1.083	0.076	0.934
Obs.	60		60		60		60	
R2	0.444		0.415		0.442		0.421	
Adj R2	0.435		0.405		0.437		0.418	
Std. Error	0.325		0.369		0.324		0.371	
F Value	368.270		321.981		346.837		359.211	
	(P = 0.000)		(P = 0.000)		(P = 0.000)		(P = 0.000)	

*** تشير إلى مستوى معنوية ٥%

تشير نتائج العمود الأول (Panel A) الى معنوية المتغير المستقل Litigious الخاص بالإفصاح عن مخاطر الأمن السيبراني باستخدام لغة التقاضي حيث أن $(t\text{-stat.} = 3.978 > 2)$ ، تشير نتائج العمود الثاني (Panel B) إلى معنوية المتغير المستقل litigious $(t\text{-stat.} = 2.649 > 2)$ بالإضافة الى ذلك، تشير نتائج العمود الثالث (Panel C) الى معنوية المتغير المستقل (t- Litigious $(t\text{-stat.} = 3.328 > 2)$) و تشير نتائج (Panel D) إلى أن $(t\text{-stat.} = 3.074 > 2)$ ، وجميعها تحمل إشارة موجبة وهو ما يشير إلى أن ارتفاع مستوى الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني يؤدي إلى زيادة التقلب في استجابة أسعار الأسهم عن إعلانات الأرباح باستخدام التداول العام، التقلب في الشراء ، التقلب في البيع، التقلب العام في الأسعار ، حيث تزداد مستوى التقلبات في العوائد غير العادية للسهم عقب إعلانات الأرباح، وهو ما يؤكد أن وجود تأثير الإفصاح السيبراني باستخدام لغة التقاضي بقدر كبيرة على وعي المستثمر وأنه يرى من خلال القوائم المالية كما أنه يحفز قراراته الاستثمارية وحجم التداول في سوق الأوراق المالية

المصري للبنوك المدرجة. وتتفق الدراسة الحالية مع دراسة (Florackis, et al., 2023) في أن مقياس التقاضي كمؤشر لمخاطر الأمن السيبراني يؤثر على عوائد الأرباح بشكل سلبي.

وأخيراً يتبين عدم معنوية أي متغير من المتغيرات الضابطة، ومن ثم فلن يكون لأي منهما تأثير على المتغير التابع الخاص باستجابة أسعار الأسهم عقب إعلانات الأرباح باستخدام التقلب في التداول، التقلب في الشراء، التقلب في البيع، التقلب العام في الأسعار، وبناء على النتائج السابق عرضها يمكن قبول الفرض الإحصائي الثالث للدراسة على الشكل البديل التالي: يوجد تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

وفى هذا السياق تتفق نتائج الدراسة الحالية مع ما توصلت إليه الدراسات السابقة ، حيث بحثت دراسة (Hansson, 2020) في أثر إعلانات الأرباح ودفع توزيعات الأرباح على أسعار الأسهم وفي معرفة ما إذا كانت هذا الأثر يدل على كفاءة السوق خلال الفترة من ٢٠١٠ إلى ٢٠٢٠، وأظهرت نتائج الدراسة أن كلاً من إعلانات الأرباح ودفعات توزيع الأرباح لهما تأثير سلبي كبير على أسعار الأسهم، حيث يرجع سبب الأثر السلبي للإعلان عن الأرباح هو انخفاض توقعات المستثمرين فيما يتعلق بالأرباح المستقبلية.

٤. النتائج والتوصيات والمقترحات البحثية

بناء على ما تم عرضه في الإطار النظري وما تم استنتاجه الباحث من التحليل الإحصائي للدراسة يمكن عرض أهم النتائج والتوصيات على النحو التالي:

١. تؤثر إعلانات الأرباح ودفعات توزيع الأرباح بشكل سلبي كبير على أسعار الأسهم، حيث يرجع سبب الأثر السلبي للإعلان عن الأرباح إلي انخفاض توقعات المستثمرين فيما يتعلق بالأرباح المستقبلية.

٢. أوضحت النتائج النظرية أن تقلبات عوائد الأسهم تعد من المخاطر التي يواجهها المستثمرون في أسواق الأسهم العالمية، ويصعب قياس تلك التقلبات بسبب تعدد وتنوع العناصر التي تؤثر في حركة الأسواق.
٣. توصلت الدراسة الحالية إلى أن أهم العوامل التي تؤثر في تقلبات الأسهم تتمثل في الإفصاح المحاسبي، المعلومات المستقبلية، وأن الشركات ذات جودة إفصاح منخفضة لديها تقلبات أعلى في عوائد الأسهم.
٤. يعد الانحراف بعد إعلان الأرباح (PEAD) يعد مشكلة أساسية حيث تصف استجابات أسعار الأسهم البطيئة أخبار أرباح الشركات غير المتوقعة للأشهر اللاحقة.
٥. توصلت الدراسة النظرية إلى أن جودة الإفصاح عن مخاطر الأمن السيبراني يمكن قياسها باستخدام مجموعة من المقاييس تتمثل في عدد الكلمات، القابلية للقراءة ولغة التفاضل.
٦. تعد تقلبات عوائد الأسهم مؤشر سلبي على قيمة الشركة ومدى استمرارها في السوق ومن ثم قد يترتب عليها زيادة مخاطر الشركة، ولذلك فهي تعتبر مصدر خطر وقلق لأي مستثمر.
٧. تشير نتائج التحليل الإحصائي إلى أن ارتفاع مستوى الإفصاح العام عن مخاطر الأمن السيبراني يؤدي إلى زيادة التقلب في استجابة أسعار الأسهم عن إعلانات الأرباح باستخدام التداول العام، التقلب في الشراء، التقلب في البيع، التقلب العام في الأسعار.
٨. توضح النتائج الإحصائية إلى أن الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني يؤثر على وعي مستخدمي القوائم المالية بقدر عالي، كما أنه يحفز قراراته الاستثمارية وحجم التداول في سوق الأوراق المالية المصري للبنوك المدرجة.
٩. يوجد تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح باستخدام القابلية للقراءة عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.

١٠. يؤثر الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني على وعي مستخدمي القوائم المالية بشكل كبير، كما أنه يحفز قراراته الاستثمارية وحجم التداول في سوق الأوراق المالية المصري للبنوك المدرجة.
١١. يوجد تأثير طردي ذو دلالة إحصائية لمستويات الإفصاح باستخدام لغة التقاضي عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم عقب إعلانات الأرباح.
١٢. ضرورة اتباع البنوك لإجراء تحليل مباشر للهجمات السيبرانية وتحديد مستويات التعرض لهذه الهجمات بالشكل الذي لا يؤثر على مستوى الأرباح التي تحققها البنوك ، وبما يؤدي إلى عدم خروج البنوك المصرية من الميزة التنافسية للقطاع المصرفي.

وبناء على ما تم عرضه من نتائج توصي الدراسة الحالية بضرورة توفير إطار عمل للإفصاح عن مخاطر الأمن السيبراني لكي يستطيع المستثمرون معرفة وضع المؤسسة تجاه مخاطر الأمن السيبراني، كما يجب علي المؤسسات إنشاء قسم للتصدي والتعامل مع مخاطر الأمن السيبراني مع ضرورة قيامها بتحديثه باستمرار بالإضافة إلي التدريب المستمر للعاملين بهذا القسم لصقل مهاراتهم وتوعيتهم بمخاطر الأمن السيبراني وعواقبه، وينبغي أن تلتزم الهيئة العامة للرقابة المالية الشركات بالمزيد من الإفصاحات المرتبطة بمخاطر الأمن السيبراني وفرض عقوبات علي الشركات في حالة تخلفها عن ذلك.

كما توصي الدراسة بإجراء المزيد من المقترحات البحثية في أثر التوقيت المعلوماتي لإفصاح الشركات عن مخاطر الأمن السيبراني علي كفاءة الاستثمار، أثر الإفصاح عن مخاطر الأمن السيبراني علي تكلفة رأس المال وعلي العلاقة بين قرار منح الائتمان والاستثمار بالأسهم، بالإضافة إلى ذلك تقديم إطار موسع لدور تقارير التآلفات الرقابية في التنبؤ بالمعلومات المستقبلية لمخاطر الأمن السيبراني وانعكاسه على قيمة المنشأة .

قائمة المراجع

المراجع باللغة العربية:

شرف، إبراهيم أحمد إبراهيم (٢٠٢٣) ، أثر الإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين – دراسة تجريبية ، مجلة الإسكندرية للبحوث المحاسبية، قسم المحاسبة والمراجعة، العدد الأول ، المجلد ٧ ، ٢٠٢٣، ٢١١-٢٨١.

علي، هبه جمال هاشم. (٢٠٢٣). منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي، *المجلة العلمية للدراسات والبحوث المالية والتجارية*، كلية التجارة، جامعة دمياط، ٤(٢) ، ٥٨-١.

فرج، هاني خليل(٢٠٢٢)، " أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الامن الإلكتروني على قرارات الاستثمار بالأسهم – دراسة تجريبية"، *مجلة المحاسبة والمراجعة* ، مجلة دولية تصدر عن كلية التجارة جامعة بنى سويف بالشراكة مع اتحاد الجامعات العربية، العدد ١١ ، ١٢٩-٢٠٩.

متولى ، مصطفى زكي حسين & غريب ، حسين عبد العال سالم. (٢٠٢٢). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية. *المجلة العلمية للدراسات المحاسبية، كلية التجارة ، جامعة قناة السويس*، ٤(٤) ، ٢٤٥-٣٢٨.

المر ، نورهان علي محمد (٢٠٢٢). قياس تأثير الإفصاح الإلزامي للمسئولية الاجتماعية للشركات على استجابة أسعار الأسهم لإعلانات الأرباح بالشركات المصرية المدرجة بالبورصة. *المجلة العلمية للدراسات المحاسبية، كلية التجارة ، جامعة قناة السويس* ، ٤(٣) ، ٩٥-١٦٢.

المر، نرمين علي محمد. (٢٠٢٤). استخدام تقنيات تعلم الآلة للتنبؤ بعوائد الأسهم وأثر ذلك على الإفصاح عن المعلومات المستقبلية. *المجلة العلمية للدراسات والبحوث المالية والتجارية*، كلية التجارة ، جامعة دمياط ، ٥(١) ، ١١٢٥-١١٧٧.

المراجع باللغة الإنجليزية:

- Andreadis, L., Kalotychou, E., Louca, C., Lundblad, C. T., & Makridis, C. (2022). Cyberattacks, Media Coverage and Municipal Finance. *Media Coverage and Municipal Finance (October 14, 2022)*.
- Anwar, N. A. M., Kamarudin, F., Noordin, B. A. A., Hussain, H. I., & Mihardjo, L. W. (2021). Disclosure level and quality effect of forward-looking information on firm's stock return: The moderating effect of ownership structure. *Transformations in Business & Economics, 20(1)*.
- Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership & Control, 15(2)*, 70-83.
- Asem, E. (2022). Are dividend changes exploited in the equity market?. *The Quarterly Review of Economics and Finance, 85*, 125-133.
- Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cyber security disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy, 41*, 1-15.
- Barth, M. E., Landsman, W. R., Raval, V., & Wang, S. (2020). Asymmetric timeliness and the resolution of investor disagreement and uncertainty at earnings announcements. *The Accounting Review, 95(4)*, 23-50.
- Berkman, H., Jona, G. Lee, and N. Soderstrom. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy 37 (6): 508–526*.

- Blankespoor, E., Dehaan, E., Wertz, J., & Zhu, C. (2019). Why do individual investors disregard accounting information? The roles of information awareness and acquisition costs. *Journal of Accounting Research*, 57(1), 53-84.
- Bonsall, S. B. IV, Leone, A. J., Miller, B. P., & Rennekamp, K. (2017). A plain English measure of financial reporting readability. *Journal of Accounting and Economics*, 63(2-3), 329-357.
- Calderon, T. G., and L. Gao. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing* 25 (1): 24-39.
- Calderon, T., and L. Gao. (2022). Comparing the cybersecurity risk disclosures of U.S. and foreign firms. *Journal of Emerging Technologies in Accounting* .19 (2): 61-79.
- Cao, H., Phan, H. V., & Silveri, S. (2023). Data Breach Disclosures and Stock Price Crash Risk: Evidence from Data Breach Notification Laws. *Available at SSRN 4393481*.
- Celeny, D., & Maréchal, L. (2023). Cyber risk and the cross-section of stock returns. *Available at SSRN 4587993*.
- Chatterjee, C., & Tiwari, S. (2022). Dividend reduction and stock price reaction in Indian market: is there a role of share repurchase?. *Journal of Indian Business Research*, 14(4), 447-471.
- Chatterjee, C., Dutta, P., & Basu, S. (2021). Evidence-based Stock Price Behaviour Around Cash Dividend Announcements in an Emerging Market Set-up. *Global Business Review*, 1-18.

- Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199-224.
- Chen, X., Diao, X., & Wu, C. (2022). Heterogeneous investor attention and post earnings announcement drift: Evidence from China. *Economic Modelling*, 110, 1-18.
- Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cyber security risk disclosure through textual analysis and factor analysis. *Journal of information Systems*, 35(2), 179-194.
- Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis*, 65, 1–18.
- Deloitte. (2020). Cybersecurity and the role of internal audit. An urgent call to action. Available at: <https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html>.
- DiStaso, M. W. (2018). Communication Challenges in Cybersecurity. *Journal of Communication Technology*, 1(1), 43-60 .
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, 36(1), 351-407.
- Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: a matter of timing?. *Management Science*, 68(10), 7298-7322.

- Fonou-Dombeu, N. C., Mbonigaba, J., Olarewaju, O. M., & Nomlala, B. C. (2022). Earnings quality measures and stock return volatility in South Africa. *Future Business Journal*, 8(1), 1-15.
- Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, 33(3), 183-200.
- Gao, L., Calderon, T. G., and Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38. 1-22.
- Grove, H., and Clouse, M. (2020). Financial and non-financial fraud risk assessment. *Journal of Forensic and Investigative Accounting*, 12(3), 422–441.
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834.
- Hansson, F. (2021). How does dividend events affect stock prices?: An event study on market efficiency.
- Harris, D., Kuzey, C., Naaman, C., & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt?. *Journal of Forensic and Investigative Accounting*, 15(2), 192-212
- Hasan, F., Kayani, U. N., & Choudhury, T. (2023). Behavioral risk preferences and dividend changes: exploring the linkages with prospect theory through empirical analysis. *Global Journal of Flexible Systems Management*, 24(4), 517-535.

- Hsu, F. J., & Chen, S. H. (2020). Does corporate social responsibility drive better performance by adopting IFRS? Evidence from emerging market. *Journal of Computational and Applied Mathematics*, 371, 1-35.
- Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. *European business review*, 26(2), 106-121.
- Jackson, S., Vanteeva, N., and Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from U.S firms. *Journal of the Association for Information Science and Technology*, 70(11), 1277–1289
- Jensen, J., & Paine, F. (2023). Municipal Cyber Risk. *Available at SSRN 4588006*.
- Jeong, K. H., & Choi, S. U. (2019). Does real activities management influence earnings quality and stock returns in emerging markets? Evidence from Korea. *Emerging Markets Finance and Trade*, 55(12), 2834-2850.
- Jiang, W., J. Legoria, K. J. Reichelt, and S. Walton. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems* 36 (1): 151–180.
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*.139. 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.
- Kelton, A., & Yang, Y. W.(2023). Understanding Cybersecurity Breach Contagion Effects: The Role of the Loss Heuristic, Managerial Ability, and Internal Controls. *Managerial Ability, and Internal Controls*.1-39.
- Khan, F., Jan, S. U., & Khan, H. (2020). Does Dividend Policy Determine Stock Price Volatility?(A Case Study of Malaysian Manufacturing Sector). *Global Policy and Governance*, 9(1), 67.
- Kumar, D., Sarangi, P. K., & Verma, R. (2022). A systematic review of stock market prediction using machine learning and statistical techniques. *Materials Today: Proceedings*, 49, 3187-3191.
- Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, 53(2), 413-455.
- Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40-55.
- Lo, K., Ramos, F., & Rogo, R. (2017). Earnings management and annual report readability. *Journal of Accounting and Economics*,63(1), 1–25
- Mall, P., & Gupta, K. (2019). Impact of merger announcements on stock returns of acquiring firms: Evidence from INDIA. *Journal of Commerce & Accounting Research*, 8(1), 46-53.

- Marotta, A., & Madnick, S. (2020). Analyzing the interplay between regulatory compliance and cybersecurity. Available at SSRN 3542563.
- Martins, A. I. (2022). *Earnings prediction using machine learning methods and analyst comparison*, Dissertation submitted in partial fulfilment of requirements for the MSc in Finance, at the Universidade Católica Portuguesa, 1-59
- Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, 76(2), 131-140.
- Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter?. *Journal of Accounting in Emerging Economies*, 13(2), 217-239.
- McEnroe, J. E., & Mindak, M. (2020). An empirical analysis of an application of an alternative measurement model on international accounting standard 33, earnings per share. *Accounting Research Journal*.33(2),1-10.
- Pacheco-Paredes, A., & Wheatley, C. M.(2022), Do Auditors Consider Cybersecurity Insurance in Pricing Audits?. Available at SSRN 4171153.
- Ponemon Institute. (2021). How much a data breach cost. <https://www.ibm.com/security/data-breach>.

- Rees, L., & Twedt, B. J. (2021). The Incremental Value Relevance of Media Coverage of Earnings Announcements: Evidence from the Trading of Short Sellers. *Accounting Horizons*, 35(4), 143-165.
- Remeis, K. (2023). Board Gender Diversity and Cybersecurity Disclosure Characteristics.2-20.<https://scholars.unh.edu/cgi/viewcontent.cgi?article=1764&context=honors>.
- Rjiba, H., Saadi, S., Boubaker, S., and Ding, X. S. (2021). Annual report readability and the cost of equity capital. *Journal of Corporate Finance*, 67. 1-70.
- Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. *European Accounting Review*, 1-28.
- Securities and Exchanges Commission – SEC (2011). CF Disclosure Guidance: Topic No. 2
- Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, 27(4), 1049-1071.
- Smith, T. J., Higgs, J. L., and Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems*, 33(2), 177–204.
- Sun, Y. V., Liu, B., & Prodromou, T. (2022). The determinants of the COVID-19 related stock price overreaction and volatility. *Studies in Economics and Finance*, 39(1), 125-149.

- Swift, O., Colon, R., and Davis, K. (2020). The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures. *Journal of Forensic and Investigative Accounting*, 12(2), 197–212.
- Temirov, A., Urinov, B., Zakirova, G., & Yuldashova, G. (2023). Impact of the dividend policy of joint-stock companies on the regulation of the stock price in the Republic of Uzbekistan. In *E3S Web of Conferences*, 402,1-9.
- Teodósio, J., Madaleno, M., & Vieira, E. (2022). Corporate governance effects on market volatility: Empirical evidence from Portuguese listed firms. *Revista Brasileira de Gestão de Negócios*, 24, 159-174.
- Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 1-15.
- Truong, P. (2023). Peer Effects and Disclosure Timing: Evidence from Earnings Announcements. *The Accounting Review*, 98(3), 427-458.
- Tsafack, G., Becker, Y., & Han, K. (2023). Earnings announcement premium and return volatility: Is it consistent with risk-return trade-off?. *Pacific-Basin Finance Journal*, 79, 1-21.
- Tsang, R. C., Baldwin, A. A., Hair, J. F., Affuso, E., & Lahtinen, K. D. (2023). The Informativeness of Sentiment Types in Risk Factor Disclosures: Evidence from Firms with Cyber security Breaches. *Journal of Information Systems*, 37(3), 157-190.
- Van Zyl, W., & Uliana, E. (2022). Fixing diluted earnings per share: Recognizing the dilutive effects of employee stock options. *Accounting & Finance*, 62(2), 2993-3019.

- Wang, T., J. C. Yen, and K. Yoon. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. *International Journal of Accounting Information Systems* .46.1-14.
- Widiastuti, H., Utami, E. R., & Purnamasari, E. (2022). Forward-looking information disclosure and firm value in the pandemic ERA. *Jurnal Riset Akuntansi Kontemporer*, 14(2), 261-269.
- Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cyber security risk management reporting framework. *International Journal of Accounting & Information Management*.28(1).167-183.