قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشأة "دراسة تطبيقية"

إعـــــداد

الباحث/ عمرو عادل عبدالفتاح موسى

مدرس مساعد بقسم المحاسبة والمراجعة
كلية التجارة – جامعة مدينة السادات

إشـــــراف

أ.د/ عبدالحميد أحمد أحمد شاهين

أستاذ المراجعة

رئيس قسم المحاسبة وعميد الكلية السابق

كلية التجارة- جامعة مدينة السادات

أ.م.د/ محمد موسى على شحاتة

أستاذ المحاسبة المساعد

رئيس قسم المحاسبة ووكيل الكلية لشؤون الدراسات العليا والبحوث
كلية التجارة- جامعة مدينة السادات

د/ مروة أحمد عبدالرحمن البحيري

مدرس بقسم المحاسبة والمراجعة
كلية التجارة- جامعة مدينة السادات

مستخلص البحث:

سعى البحث إلى تسليط الضوء على آليات الإفصاح الالكتروني عن المخاطر السيبرانية، واستخلاص إطار محاسبي لآليات الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها، ودراسة وتحليل الآثار الجوهرية لهذه الإفصاحات على القوائم المالية والتقارير السنوية والإفصاحات ذات الصلة، وبيان أثر تبني محاور الإفصاح عن بنود هذا المؤشر علي قيمة المنشأة، وذلك **كدراسة تطبيقية** على عينة نهائية لعدد (٨) **بنوك** و(٦) شركات **بقطاع الاتصالات والاعلام وتكنولوجيا المعلومات** تكون **(٤٢)** مشاهدة للسنوات **(٢٠١٩ – ٢٠٢١)**، وتوصلت **نتائج البحث** إلى أن شركات العينة تفصح عن المخاطر السيبرانية بمتوسط عام بلغ **(٢٤,٣٥)** وبنسبة إفصاح بلغت **(٤٦٪)**، ووجود علاقة **ارتباط إيجابية معنوية** بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة، **وأسفرت نتائج تحليل الانحدار** عن وجود **أثر ذا دلالة احصائية** للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة، ووجود **اثر إيجابى** لكل من ربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات على قيمة المنشأة، و**عدم وجود** أثر معنوى **لحجم الشركة** علي قيمة المنشاة، **وأوصى البحث** بضرورة تبني الشركات المزيد من الافصاح و الشفافية في التقارير والقوائم المالية، لإعلام مستثمريها بكافة المخاطر السيبرانية المحتملة والفعلية الجوهرية، التي قد تؤثر على أعمالها ونتائجها المالية، والإفصاح عن سيناريوها مواجهة المخاطر السيبرانية وإدارتها، والتخفيف من حدتها، فضلاً عن **إصدار معيار محاسبي** لتنظيم القياس والافصاح عن المخاطر السيبرانية، وآثارها الحالية والمحتملة على الفروض والمبادئ المحاسبية وعلى القوائم والتقارير المالية السنوية.

Abstract:

The research sought to shed light on the mechanisms of electronic disclosure of cyber risks, to derive an accounting framework for the mechanisms of electronic disclosure of cyber risks and the governance of their management, to study and analyze the essential effects of these disclosures on the financial statements, annual reports and related disclosures, and to demonstrate the impact of adopting the axes of disclosure of the items of this indicator on The value of the establishment, as an applied study on a final sample of (8) banks and (6) companies in the communications, media and information technology sector, which is (42) observations for the years (2019-2021), and the results of the research concluded that the sample companies disclose cyber risks with a general average of (24.35), with a disclosure rate of (46%), and the existence of a significant positive correlation between the electronic disclosure of cyber risks and the value of the establishment. The company, the degree of financial leverage and the quality of corporate governance on the value of the establishment, and the absence of a significant impact of the size of the company on the value of the establishment, and the research recommended the need for companies to adopt more disclosure and transparency in reports and financial statements, to inform their investors of all potential and actual substantial cyber risks that may affect their business And its financial results, and the disclosure of its scenarios for confronting and managing cyber risks, and mitigating their severity, as well as issuing an accounting standard to regulate the measurement and disclosure of cyber risks, and their current and potential effects on assumptions and accounting principles and on financial statements and reports.

أولاً: الإطار العام للبحث

١- مقدمة البحث:

أدى ظهور الأدوات الحديثة في نظم وتكنولوجيا المعلومات الرقمية إلى ترابط غير مسبوق، ويمكن أن تؤثر على قيمة المنشأة عن طريق زيادة التدفقات النقدية المتوقعة وخفض تكلفة رأس المال(Salvi et al., 2021, p 438). وأن الاعتماد على الاستعانة بمصادر خارجية لتكنولوجيا المعلومات، يزيد من تعرض المنشآت للحوادث السيبرانية التي يسببها الطرف الثالث، ويجب أن تعكس أسعار الأسهم جميع المعلومات الجوهرية للمنشأة حول المخاطر السيبرانية التي تتعرض لها (Benaroch, 2021, p1-3).

وتتزايد المخاطر السيبرانية وتشكل تهديداً محتملاً للشركات، خاصةً بالنسبة للشركات المدرجة بالبورصة، حيث يمكنها خلق تأثير طويل الأجل على أدائها المالي، وبالتالي على القيمة السوقية للمنشأة (Ali and Lai, 2022, p689). وتمثل القيمة غير الملموسة- قيمة الأصول غير المادية بطبيعتها- الآن ٩٠٪ من قيمة الأصول في المنشآت، حيث تضاعفت أكثر من ثلاثة أضعاف في مؤشر(S&P500)خلال الـ٣٥عاماً الماضية، وخلال جائحة(COVID-19)، اتخذت المنشآت تحولاً سريعاً لرقمنة أصولها، وربما يكون أهم أصل غير ملموس في تحديد قيمة المنشأة اليوم هو البيانات - سواء كانت بيانات شخصية أو معلومات مالية أو بيانات أمان، ومع نمو المنشآت، تنمو قيمتها غير الملموسة أيضاً، مما يزيد من التأثير المحتمل لخرق الأمن السيبراني، وفي هذا السياق، تزداد الجريمة السيبرانية لتحقيق الربح الاقتصادي(WEF, 2022, p3). وتؤثر الهجمات السيبرانية على قيمة الشركة، من خلال الطرق التالية:(التكلفة المالية المباشرة وتكلفة الأضرار المادية، والخسائر الناجمة عن سرقة الملكية الفكرية، والضياع والخسارة الناجمة عن إتلاف أو حذف البرامج والبيانات، وانقطاع الأعمال وتكاليف الاسترداد بعد الهجوم/ التعافي من التخلف عن السداد، وفقدان العميل والقدرة السعرية، وتزداد تكلفة الغرامات التنظيمية والتسوية القانونية، فضلاً عن تكلفة الأقساط المستقبلية، والتكلفة المحتملة للمسؤولية تجاه الغير، والطرف الثالث(Tong, 2023, p2).

ومع التطور التكنولوجي في مجال الاتصالات والإنترنت، أصبحت المواقع الالكترونية قنوات مهمة للشركات للإفصاح المحاسبي الفوري وبتكاليف أقل والوصول إلى نطاق أوسع من المستخدمين، وذلك بالمقارنة بوسائل الإفصاح التقليدية مثل التقارير السنوية الورقية، بما خلق الفرصة للشركات لتوسيع نطاق الإفصاح المحاسبي وتنويع طرق عرض المعلومات باستخدام ملفات الصوت والفيديو وغيرها، بما يساهم في تحسين جودة الإفصاح المحاسبي وجذب المزيد من المستثمرين (الصاوي، ٢٠٢٢؛ Khlifi, 2022).

وفي **١١مارس٢٠٢٢**، أصدرت (SEC)تعديلات لتعزيز وتوحيد متطلبات الإفصاح الالكتروني المتعلقة بإدارة الأمن السيبراني، والإبلاغ عن الحوادث السيبرانية والتقارير الدورية من قبل المنشآت لإعلام المستثمرين بشكل أفضل بإدارة مخاطر المنشأة واستراتيجيتها وحوكمتها المتعلقة بالمسائل الإلكترونية، وتقديم إخطار في الوقت المناسب بحوادث الأمن السيبراني الجوهرية، وبموجب القواعد المقترحة يُطلب من المنشآت العامة ما يلي:(الإبلاغ عن حادثة جوهرية للأمن السيبراني في غضون أربعة أيام عمل في النموذج(8-K) أو النموذج(6-K) الإفصاح عن سياسات وإجراءات الأمن السيبراني لتحديد وإدارة المخاطر السيبرانية ودور الإدارة في تقييم المخاطر السيبرانية وتحليلها، واقترحت التعديلات ضرورة تقديم تقارير سنوية الزامية، في النموذج(10-K) أو النموذج(20-F)، لتوفير تحديثات بشأن أي تغييرات جوهرية لحوادث الأمن السيبراني المبلغ عنها في النموذج(10-K) والنموذج(10-Q) أو النموذج(20-F)، والإفصاح في تعليقات الإدارة عن أي خبرة في مجال الأمن السيبراني لمجلس إدارتها، فضلاً عن تقديم إفصاحات الأمن السيبراني **بلغة تقارير الأعمال الموسعة في Inline XBRL للوصول إليها بسهولة**، وأرفقت(SEC) هذه الافصاحات بقاعدة تشريعية قانونية متمثلة بقانون الأوراق لمخاطر وحوادث الأمن السيبراني الأمريكي(akingump ,2022,p1; Trautman and Newman, 2022, p7).

وأكدت دراسة(Jiang et al., 2022)على أن الإفصاح الإلكتروني عن طبيعة المخاطر السيبرانية وإدارتها، إحدى الطرق التي يمكن من خلالها التواصل مع أصحاب المصالح، وينبغي أن تنعكس المخاطر السيبرانية المؤكدة والمحتملة، وردود الفعل السوقية المتعلقة بالاختراق على توفير إفصاحات إضافية

للمنشأة في القوائم والتقاريرالسنوية. ويمكن أن تؤثر المخاطر السيبرانية بشكل جوهري على العمليات التجارية وسلامة التقارير المالية(Ramírez et al., 2022,p8).

وإن إعداد التقارير المالية عبر الإنترنت (IFR) هو ممارسة لنقل المعلومات المالية وغير المالية عبر الإنترنت، وتهدف ممارسة IFR إلى توفير قناة لإيصال المعلومات المتاحة على موقع الشركة الإلكتروني للمستثمرين لدعمهم في تقييم أداء الشركة وقرارات الاستثمار، وأن الإفصاح عبر الإنترنت مهم لمنظمي الأوراق المالية وواضعي معايير المحاسبة ومجتمع المحاسبة الأوسع Hussein & (Nounou, 2022, p842).

ويعتبر المنظمون مثل PCAOB و SEC أن هذا مجال يثير قلقاً متزايداً ويركزون اهتمامهم على كيفية معالجة و مراقبة المخاطر السيبرانية في التقارير المالية، وتقديم التقارير إلى مستخدمي البيانات المالية(Bricker et al., 2022). وصرح المعهد الأمريكي للمحاسبين القانونيين(AICPA,2018, p1)بأنّ الأمن السيبراني هو أحد أهم القضايا التي تشغل بال مجالس الإدارة في كل شركة في العالم. ووضع إطارعمل للتقرير عن هذه المخاطر، من خلال ثلاث أجزاء رئيسية من المعلومات وهي:(وصف الإدارة لبرنامج إدارة المخاطر السيبرانية للمنشأة ، وتأكيدات الإدارة بشأن فعالية ضوابط الأمن السيبراني، ورأي المراجع بشأن إفصاحات الإدارة)(الرشيدي، عباس، ٢٠١٩، ص٤٤٥؛ Kelton and Pennington, 2021, p.137). وأوضح المعهد الإندونيسي للمحاسبين القانونيين المعتمدين (IAPI) أن للمحاسبين دوراً مهماً في عالم الأعمال والحكومة في تحديد تحديات مخاطر الجريمة السيبرانية والتغلب عليها(Asauri, 2022, p4). وإذا قررت المنشآت أنها لا تستطيع الحد بشكل كافٍ من تعرضها للمخاطر السيبرانية من خلال تحسين أمان بياناتها، فقد تختار تغيير ممارسات الإفصاح المالي لتقليل التكاليف المرتبطة بإمكانية الاضطرار إلى الإفصاح عن خرق البيانات في المستقبل(Obaydin et al., 2021, p4).

وورد في تقرير مجلس التقارير المالية(FRC)الصادر في أغسطس ٢٠٢٢، أن الأمن الرقمي والأنظمة والعمليات والبيانات الرقمية وبالتالي مخاطر الأمن الرقمي، أمراً أساسياً لاستمرارية الأعمال والمرونة وخلق القيمة، ويجب أن يوفر الإفصاح عن هذه المجالات المعلومات ذات الصلة للمستثمرين وأصحاب المصلحة الآخرين، لمساعدتهم في تقييم قدرة المنشأة على الاستمرارية والمرونة(FRC, 2022, p3). ومع زيادة وعي أصحاب المصلحة بالمخاطر السيبرانية، تميل المنشآت إلى الإفصاح الالكتروني عن المعلومات المتعلقة بالمخاطر السيبرانية(Yang et al., 2020, p178).

وفي الواقع، أدت الحاجة إلى إدارة سرية المعلومات ونزاهتها وتوافرها إلى قيام مجالس إدارة الشركات بالنظر في التهديدات السيبرانية، وبالتالي أصبح الأمن السيبراني مؤخراً جزءاً من الفهم السائد ومجال التحقيق من قبل حوكمة الشركات؛ على الرغم من أن الوقت قد حان لأن تركز الحكومة والمؤسسات والشركات وأصحاب المصلحة الآخرون على استراتيجيات الأمن السيبراني وتطبيقاتها في المحاسبة، إلا أن الإدارة العليا لا تزال لا تأخذ في الاعتبار مخاطر الأمن السيبراني على مستوى مجلس الإدارة، وهناك **غموض مستمر** حول من المسؤول عن الأمن السيبراني في المنظمة (من الناحية المثالية، يجب أن يكون كبار المديرين التنفيذيين مسؤولين)، وستستجيب معايير المحاسبة المستقبلية لضرورة الإفصاح مع ضرورة حماية البيانات الحساسة(Napolitano, 2023, p2).

وبالتالي، في المستقبل القريب، يمكن أن يحل إعداد التقارير المالية المستمرة عبر الإنترنت محل التقارير المالية الدورية، في سيناريو إعداد تقارير قاعدة البيانات المركزية، يمكن لجميع المستخدمين " (أولئك المهتمين بالبيانات المالية للمؤسسة) الوصول إلى قاعدة البيانات المركزية للشركة في أي وقت عبر الويب(Napolitano, 2023, p17). ويتلقى متخصصو المحاسبة والمراجعة أيضاً معلومات محاسبية في الوقت الفعلي من خلال استخدام الإنترنت، وتقلل الاتصالات الإلكترونية العالمية بشكل كبير من الفارق الزمني بين حدوث المعلومات المحاسبية ونقلها إلى قسم المحاسبة، ونتيجة لذلك، تكون المعلومات المحاسبية التي يتم التقاطها تلقائياً دائماً في الوقت المناسب وحديثة، وهناك تهديدات سيبرانية كبيرة لتشغيل المؤسسة بسبب الحاجة إلى الاتصال الدائم لأجهزة الاستشعار التكنولوجية بالإنترنت(Desyatnyuk et al., 2022, p361).

وكنتيجة حتمية لما سبق، تقوم المنشآت بتنفيذ التدابير لمواجهة المخاطر السيبرانية، من خلال تبني أنظمة تكنولوجية مؤمنة ومحدثة، مما يتطلب تقديم إفصاحات أكثر شمولاً عن أي مخاطر سيبرانية

والمعلومات المتعلقة باستراتيجيات وسيناريوهات تخفيفها وإدارتها، مما يؤدي إلى حدوث زيادة في قيمة المنشأة، ويوجد أثر إيجابي بين القيمة السوقية للمنشأة ومقياس الوعي بالأمن السيبراني، والمنشآت التي تفصح عن المزيد من قضايا الأمن السيبراني تحظى بتقدير أعلى من قبل السوق (Berkman et al., 2018, p.509-510).

وفي ضوء ماسبق، يسعي البحث إلى تسليط الضوء على آليات الإفصاح الالكتروني عن المخاطر السيبرانية، وإستخلاص إطار محاسبي لآليات الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها، ودراسة وتحليل الآثار الجوهرية لهذه الإفصاحات على القوائم المالية والتقارير السنوية والإفصاحات ذات الصلة، وبيان أثر تبني محاور الإفصاح عن بنود هذا المؤشر علي قيمة المنشأة، وبما يتلائم مع بيئة الأعمال المصرية في ضوء التحول الرقمي والحوكمة والمرونة السيبرانية والرقمنة، وذلك كدراسة تطبيقية.

٢- مشكلة وتساؤلات البحث:

يعد تغيير نماذج الأعمال المصرفية من خلال إدخال الابتكارات الرقمية ذا أهمية أساسية للتطوير المستقبلي للنظام المصرفي، ولكنه في نفس الوقت يتعلق بتطوير المخاطر الحالية والجديدة للبنوك، مما يتطلب إجراء تحليل نقدي لمخاطر إدخال مختلف المنتجات والخدمات المصرفية الرقمية في مجال عمليات الدفع، وعلى هذا الأساس، تحديد الجوانب المحاسبية المحددة لهذه المخاطر، ويعتبر الإفصاح المتمايز عن التكاليف المتكبدة و / أو الخسائر المبلغ عنها من حدوث المخاطر السيبرانية في البيانات المالية للبنوك المتعلقة بالمنتجات والخدمات الرقمية، وخاصة عمليات الدفع الرقمية أمر ضروري، من أجل التحديد الصحيح وتقييم وتحليل هذه المخاطر من قبل جميع مستخدمي المعلومات المالية(Marinova, 2022, p105, 112).

وأصبح التعامل في الفضاء السيبراني أحد المخاطر الرئيسية التي يجب أن تتعامل معها الشركات من جميع الأحجام، حيث أصبحت المخاطر السيبرانية أحد أكبر أشكال المخاطر على المستوى الدولي، مما يضر بأنظمة تكنولوجيا المعلومات الخاصة بالشركات في جميع أنحاء العالم(Savaş and Karataş, 2022, p14; Poddar, 2023, p5). وتعتبر المخاطر السيبرانية هي التحدي الرئيسي في عصر الرقمنة في عالم يزداد تعقيداً وتطوراً، وتعتبر مصدر قلق كبير في المنشآت، ويمكن أن تؤثر بشكل جوهري على قيمة المنشأة لمستثمري رأس المال(Mitts and Talley, 2019, p1). وأشار الإتحاد الدولي للمحاسبين في تقريره(IFAC, 2019) أن التهديدات والمخاطر السيبرانية أصبحت محط تركيز المنشآت والحكومات على مستوى العالم، وتسبب خسائرمالية كبيرة والإضراربسمعة المنشأة؛ إذا لم يكن لديها خطة أمان إلكترونية مناسبة، وينبغي وضع خطط واجراءات لمواجهة وإدارة هذه المخاطر تتناسب مع حجم المنشأة للتخفيف من حدتها وآثارها. وينمو عدد الحوادث السيبرانية بنسبة ٢٥٪ ويزداد عدد المنشآت التي تقع ضحية بنسبة ٢٢٪ سنوياً(Kolesnikov et al., 2022, p1). ونشر(Audit Analytics)في أبريل ٢٠٢٢ تقريراً جديداً بشأن اتجاهات الإفصاح الإلكتروني عن الحوادث السيبرانية، ويشير التقرير إلى أنه في عام ٢٠٢١، كانت هناك زيادة بنسبة ٤٤٪ في عدد المخالفات التي تم الإفصاح عنها، من ١٣١ في عام ٢٠٢٠ إلى ١٨٨ في عام ٢٠٢١(Posner, 2022, p1) .

وبالنسبة للأوضاع في البيئة المصرية، فإن ٦١٪ من المنشآت المصرية ليس بها حماية كافية للمعلومات، وبلغت خسارتها المالية نحو**٣,٧٨**مليون دولار(المركز المصري للدراسات الاقتصادية، ٢٠١٩). وصنف تقرير شركة (Check Point's, 2021, p. 7- 16; 37)العالمية أن مصر تقع ضمن الدول ذات المخاطر الأعلى في المخاطر السيبرانية، ووجود إحصائيات غير كافية حول حجم المخاطر والتهديدات السيبرانية والسلامة المعلوماتية في مصر، ولقد أدت جائحة كورونا إلى زيادة معدل هجوم البريد الإلكتروني للتصيد الاحتيالي بنسبة ٢٢٠٪. ووفقاً للتقرير السنوى الصادرعن المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات EG-CERT لعام ٢٠١٩/٢٠١٨ أن أكثر القطاعات تعرضاً للحوادث السيبرانية في مصر هو قطاع الاتصالات وتكنولوجيا المعلومات بنسبة ٤٢٪ من إجمالي الحوادث السيبرانية. وكشفت دراسة استطلاعية أجرتها Kaspersky في عام ٢٠١٨ عن أبرز الدول العربية التي تعرضت لهجمات سيبرانية على شبكاتها وأنظمتها، وجاءت مصر في المركز الثالث على مستوى القارة الأفريقية بنسبة ٥٧,٦٪. وقد تعرضت مصر للعديد من هذه الهجمات فوفقاً للتقرير الصادر

عن شركة" تريند مايكرو" عام ٢٠١٨، فإن إجمالي عدد البرمجيات الخبيثة التي إكتشفتها Kaspersky في البلاد قد وصل إلى ٢٤٢,٤١١ برمجية خبيثة خلال الربع الأخير من عام ٢٠١٧ وحده ما يمثل زيادة بنسبة ٢٥٪عن الربع الثالث من نفس العام والذي شهد اكتشاف ١٩٤,٧١٩ برمجية خبيثة(المركز العربي للبحوث والدراسات.٢٠٢٠). وبحسب المؤشر العالمي للأمن السيبراني(GCI)، والمكون من ٤٦ مؤشر مختلف، والذي يصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة، فإن مصر تقع في المرتبة الـ ١٤عالمياً والثالثة عربياً عام ٢٠١٧، وتقع في المرتبة الـ ٢٣عالمياً والرابعة عربياً عام ٢٠١٩، وعلى الرغم من أن مصر تقع في تصنيف الدول الأعلى التزاماً بالأمن السيبراني محققة (٠,٨٤٢) درجة، إلا أنها تراجعت في الترتيب العالمي (٩) مراكز وعربياً مركزاً واحداً(GCI, 2020, p57).

وتتجسد مشكلة البحث في أنه على الرغم من وجود بعض الأطر، التي تناولت المخاطر السيبرانية، بما في ذلك COBIT.5، ومعايير الآيزو وغيرها، إلا أنه لا يوجد إطار محدد لتوجيه الإفصاح الالكتروني والتقرير عن المخاطر السيبرانية، وحوكمة إدارتها وكيفية معالجة هذه المخاطر، إضافةً إلى عدم صدور أية تعليمات من قبل الهيئة العامة للرقابة المالية أو البورصة المصرية لتوجيه المنشآت للإفصاح الالكتروني عن ممارسات الأمن السيبراني والمخاطر التي تتعرض لها وحوكمة إدارتها، مما دعى إلى محاولة بناء مؤشر محاسبي مقترح للإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها على قيمة المنشأة، وذلك كدراسة تطبيقية بالبيئة المصرية.

<u>ومن ثم يمكن بلورة المشكلة البحثية في ضوء التساؤلات التالية:</u>

١- ما مدى كفاية محتوى الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها في القطاعات المصرية محل الدراسة(البنوك- تكنولوجيا المعلومات والاتصالات)؟
٢- ماهي طبيعة واتجاه العلاقة بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة؟.
٣- ما هو أثر الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها على القيمة السوقية في القطاعات المصرية محل الدراسة(البنوك- تكنولوجيا المعلومات والاتصالات)؟

٣- عرض وتحليل الدراسات السابقة:

فيما يلي نستعرض ملخصاً لأهم الأبحاث والدراسات السابقة التي تناولت المجالات المختلفة لموضوع البحث، وذلك للتوصل إلي أهم نتائجها، وهي كما يلي:

١/٣- دراسات اهتمت بالإفصاح الالكتروني عن المخاطر السيبرانية:

سعت **دراسة(Gao et al., 2020)**إلى التعرف علي ممارسات الإفصاح الالكتروني عن المخاطر السيبرانية، من خلال تحليل المحتوي والخصائص اللغوية لممارسات الإفصاح عن المخاطر السيبرانية، والتعرف على أهم العوامل التي تدفع المنشآت للإفصاح عن المخاطر السيبرانية، من تقارير 10-K لـ ١١٢ شركة من المنشآت الأمريكية العامة المدرجة في Compustat، وما مجموعه ١٣٤٤ ملاحظة لسبع قطاعات من عام ٢٠٠٧ إلى عام ٢٠١٨، **وتوصلت** إلى أن معظم الكلمات في المخاطر السيبرانية ترتبط بعمليات الإفصاح عن المخاطر المتعلقة بتعطيل الخدمة بسبب الهجمات السيبرانية(٤٠,٩٢٪)، ومخاطر فقدان البيانات السرية(٤٤,٢٠٪). في حين تناولت **دراسة(Héroux and Fortin, 2020)**فحص وتحليل طبيعة ومحتوى إفصاحات الأمن السيبراني للشركات الكندية، ومدى توافقه مع أفضل الممارسات، وتكونت عينة الدراسة من المنشآت المدرجة في مؤشر S & P / TSX 60، وتم إجراء تحليل للوثائق الصادرة بين يناير ٢٠١٧ ومنتصف ٢٠١٨، واستخدمت الدراسة تحليل المحتوى من خلال مؤشر مكون من ٤٠ بند ومقسم لسبع فئات/ **وتوصلت** إلى أن مستويات الإفصاح الالكتروني عن الأمن السيبراني منخفض، وتختلف المنشآت على نطاق واسع في مقدار التفاصيل التي تقدمها بشأن المخاطر السيبرانية وتخفيفها، وتوجد فروق ذات دلالة إحصائية بشأن المخاطر السيبرانية، وتخفيف المخاطر السيبرانية، وحوادث الأمن السيبراني المحتملة، وأن المنشآت تسعى لتجنب اللغة المعيارية في الإفصاح عن المخاطر السيبرانية والتقرير عنها.

واستخدمت **دراسة (Swift et al., 2020)** تقنيات التحليل النصي المستخدمة في الدراسات المحاسبية، وتحليل تأثير الانتهاكات السيبرانية على محتوى إفصاحات البيانات المالية، وتحليل العلاقة بين حدوث خرق والإفصاحات عن المخاطر السيبرانية، وتحديد مدى وجود اختلافات جوهرية في محتوى

الإفصاح عن الأمن السيبراني قبل الاختراق وبعده، من خلال **دراسة تطبيقية** وتحليل المحتوى على عينة نهائية من ٢٣٥ تقرير من ١٠٠٠ تقرير، لـ٤٧ شركة تعرضت لخرق سيبراني من ٢٠١١إلى ٢٠١٥، **وتوصلت** إلى وجود علاقة ذات دلالة إحصائية بين حدوث خرق للأمن السيبراني وخصائص معينة لإفصاحات الأمن السيبراني، وأن الانتهاكات السيبرانية لها تأثير كبير على طول الإفصاحات، وزيادة بنسبة ١٧,٥٪ في عدد الكلمات في عمليات الإفصاح عن الأمن السيبراني بعد الخرق، وانخفاض بنسبة ٦٢,٧١٪ في اللغة المعيارية عند مقارنة إفصاحات الأمن السيبراني السابقة للخرق بالإفصاحات التي تم إجراؤها في سنة الانتهاك والسنوات اللاحقة. واستهدفت **دراسة (Cheong et al., 2021)**إلى تحليل إفصاحات المنشآت حول المخاطر السيبرانية في قسم عوامل الخطر، وتقييم المعلومات المتعلقة بالإفصاحات في **حالتين:** خرق الأمن السيبراني والعكس، ورأي SOX 404، وتحليل محتويات الإفصاح عن المخاطر السيبرانية عندما تتعرض المنشأة لحادث أمن سيبراني أو تتلقى رأياً سلبياً عن SOX 404، **واشتملت العينة** على **٢٥١٧٩ إفصاحاً** عن المخاطر السيبرانية لـ **٤٩١٨شركة** للفترة ما بين **٢٠٠٦** و **٢٠١٧**، **وقياس الإفصاح عن المخاطر السيبرانية** من خلال تطبيق التحليلات النصية، **وأظهرت النتائج** أن كل حدث سلبي يؤثر على إفصاحات المخاطر السيبرانية للشركات، وأن المنشآت المخترقة لا توفر قدراً كافياً من الإفصاح بعد تعرضها لخرق للأمن السيبراني، وخاصةً، لا تفصح المنشآت التي تم خرقها كثيراً عن (التحكم في الحوادث الخاصة بها وتخفيف المخاطر واستمرارية الأعمال مع الإفصاح أكثر عن المخاطر الناشئة عن الطرف الثالث)، وتميل المنشآت إلى الإفصاح عن المزيد من العوامل المتعلقة بالسيطرة على الحوادث للتخفيف من الآثار السلبية.

وتمثل الهدف الرئيسي **لدراسة(Masoud and Al-Utaibi, 2022)**في تحليل العلاقة بين الإفصاح الالكتروني عن المخاطر السيبرانية وخصائص إعداد التقارير المالية، لـ**(٦٥٥شركة/سنة)**، وبإجمالي ملاحظات**(٢٧٥٤٨)**، والمخترقة(٣١٩ملاحظة)، وغير المخترقة(٢٧٢٢٩ ملاحظة)، للفترة من ٢٠٠٦ إلى ٢٠١٦، وتوصلت **النتائج** إلى أن هناك تأثيراً للإفصاح عن المخاطر السيبرانية في التقارير المالية قبل وبعد الاختراق، وهذا يعنى أن إدخال الإفصاح عن الأمن السيبراني عادة في شكل تقارير مالية، يؤدي إلى إفصاح المنشآت التي ليس لديها مخاطر جوهرية للأمن السيبراني، ويعتبر الارتباط بين الإفصاح عن المخاطر السيبرانية والأضرار المالية التي تم الإبلاغ عنها لاحقاً إيجابياً وجوهرياً. وقامت **دراسة(علي، وعلي، ٢٠٢٢)** بتحليل أثر الإفصاح عن تقرير إدارة المخاطر السيبرانية على قرار الاستثمار بأسهم المنشآت المقيدة بالبورصة المصرية، وكذلك اختبار أثر بعض الخصائص الديمغرافية(مستوى الخبرة والتأهيل العلمي للمستثمر) كمتغيرات معدلة على العلاقة محل الدراسة، ولتحقيق هدف البحث تم إجراء دراسة **تجريبية** على عينة من المستثمرين بالأسهم والمحللين الماليين في شركات السمسرة، وخلصت **الدراسة** إلى وجود تأثير إيجابي ومعنوي لتقرير إدارة المخاطر السيبرانية على قرار الاستثمار في الأسهم، كونه يضفي الثقة على أعمال المنشأة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية، مما يمكن المستثمرين من تقييم مدى قدرة المنشأة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، مما يسهم في ترشيد قرارات المستثمرين.

وركزت **دراسة (Duvenhage et al., 2022)**على تحليل ومقارنة ممارسات الإفصاح الالكتروني عن المخاطر السيبرانية داخل القطاع المصرفي وتقييم متطلبات الإفصاح في جنوب إفريقيا والصين، وتسليط الضوء على أهمية الإفصاح عن المخاطر السيبرانية في القطاع المصرفي، واستند حجم العينة إلى بنوك جنوب إفريقيا والصين "الأربعة الكبار"، واستخدمت تحليل التمايز وتحليل المحتوى للتقارير السنوية للبنوك محل الدراسة لعام ٢٠١٨، **وأظهرت النتائج** تمايز في الاختلاف بين مستويات الإفصاح عن المخاطر السيبرانية لكل دولة، وأن التقارير المالية التي نشرتها بنوك جنوب إفريقيا ذات جودة أعلى بالمقارنة مع البنوك في الصين، وبلغ مقدار الإفصاح في بنوك جنوب أفريقيا (٤٨ كلمة) متعلقة بالأمن السيبراني أكبرمن عدد الكلمات في البنوك الصينية(٧كلمات)، ولم يتم الإفصاح عن حادثة واحدة تتعلق بالمخاطر السيبرانية للسنة المالية ٢٠١٨. واعتمدت **دراسة(Chen et al., 2022)**على تحليل إفصاحات المنشآت وقياس مقدار الإفصاح عن عوامل المخاطر السيبرانية ضمن التقارير السنوية للشركات الصادرة قبل حدوث خرق البيانات مقابل بعد حدوث خرق البيانات، خلال الفترة من عام ٢٠٠٦إلى ٢٠١٨،

وباستخدام عينة من ٥٥٨ ملاحظة/سنة للشركات الربحية(التجارية)، تمثل ٢٧٩ سنة - المنشآت مقسمة إلى(٢٧٩سنة/ شركة مخترقة) و (٢٧٩سنة/ شركة غير مخترقة) بإجمالي (١,١١٦) مشاهدة للشركات(المخترقة وغير المخترقة) في فترات ما قبل الانتهاك وما بعده، وقامت الدراسة باستخدام أسلوب تحليل المحتوى لقياس مقدار الإفصاح(باستخدام عدد الكلمات)، **وتوصلت الدراسة** إلى أنه في حين أن كل من المنشآت المخترقة وغير المخترقة تزيد في المتوسط من مقدار الإفصاح عن عوامل المخاطر السيبرانية بما يتفق مع الاتجاه العالمي لإطالة إفصاحات عوامل الخطر، فإن الزيادة أكبر بشكل ملحوظ بالنسبة للشركات التي تم اختراقها مقارنة بالمنشآت غير المخترقة، ووجدت أن الزيادة في الإفصاح عن عوامل المخاطر السيبرانية لا تظهر إلا عندما تتعرض المنشأة لخرق شديد للبيانات.

وفي هذا السياق، اقترحت **دراسة(يعقوب وآخرون, ٢٠٢٢)**مؤشر للإفصاح عن المخاطر السيبرانية ضمن المعلومات المفصح عنها في التقارير السنوية، في ظل غياب التعليمات المنظمة لهذا النوع من الافصاحات، وتم بناء مؤشر للإفصاح المحاسبي عن المخاطر السيبرانية، وفقاً للمتطلبات الدولية الصادرة عن الهيئات المهنية والتشريعات الأجنبية والعربية، واقتصرت **عينة البحث** على أربعة بنوك مدرجة في البورصة خلال الفترة من ٢٠١٩-٢٠٢٠، و**توصلت** الدراسة إلى وجود اختلافات في افصاح البنوك عينة الدراسة وفق المؤشر المقترح للإفصاح عن المخاطر السيبرانية، **وأوصت** بضرورة تبني المؤشر المقترح للإفصاح عن المخاطر السيبرانية في البيئة العراقية. **وأخيراً**، استهدفت **دراسة (Ramírez et al., 2022)** إنشاء مؤشر إفصاح يسمح بتحليل نطاق الإفصاح عن معلومات الأمن السيبراني الطوعية والإلزامية، وتوفير أداة جديدة لقياس محتوى الإفصاح عن الأمن السيبراني التي تنطبق في أي صناعة، وتقييم نطاق الإفصاح في أمريكا اللاتينية، من خلال التركيز على تقنية **تحليل المحتوى** المستخدمة في فحص وتحديد معلومات الأمن السيبراني التي تم الإفصاح عنها في التقارير السنوية من ٢٠ نموذجاً سنوياً للشركات ذات أعلى قيمة سوقية في الأوراق المالية في دول الأرجنتين والبرازيل وشيلي وكولومبيا والمكسيك وبيرو خلال الفترة (٢٠١٦-٢٠٢٠) ضمن **أربع قطاعات**(الطاقة، المالي- القطاع التقديري للمستهلكين- المواد)، **وتسلط النتائج** الضوء على أن أعلى نسبة إفصاح ذات صلة هي الأرجنتين، ويرجع الفضل في الإفصاحات الأكثر شمولاً إلى القطاع المالي؛ ويمثل بُعد الاستراتيجية أكبر وزن في درجة المؤشر.

وأخيراً، استهدفت دراسة**(شرف، ٢٠٢٣)**اختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، وأيضاً اختبار أثر بعض السمات النوعية للمستثمر (الجنس، والعمر، ومستوي التأهيل العلمي) كمتغيرات معدلة للعلاقة محل الدراسة، من خلال إجراء دراسة تجريبية علي عينة من ١٠٨ من أعضاء هيئة التدريس وطلبة الدراسات العليا بكليات التجارة بالجامعات المصرية، كممثلين للمستثمرين غير المحترفين، وقد خلصت الدراسة في شقها التجريبي إلى وجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين، ووجود تأثير معنوي لكل من (الجنس، والعمر، ومستوي التأهيل العلمي للمستثمر) علي العلاقة بين إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين.

٢/٣- دراسات اهتمت بالعلاقة بين الإفصاح الالكتروني عن المخاطر السيبرانية وقيمة المنشأة:

استهدفت **دراسة(Amir et al., 2018)**تحليل الحوافز لدي المديرين لحجب المعلومات السلبية، من خلال **دراسة تطبيقية** لـ٢٧٦ من حوادث(رفض الخدمة) لـ١٥٦ شركة مساهمة بين عامي ٢٠١٠ و ٢٠١٥، **وتوصلت** إلى أن الهجمات السيبرانية التي لم يتم الإفصاح عنها ترتبط بانخفاض ما يقرب من(٣,٦ ٪) في قيم الأسهم في الشهر الذي تم فيه اكتشاف الهجوم، والهجمات السيبرانية التي تم الإفصاح عنها ترتبط بإنخفاض أقل بكثير بنسبة(٠,٧٪)، وانخفاض قيم حقوق الملكية بنسبة(٠,٣٣٪) في الأيام الثلاثة و(٠,٧٢٪)في الشهر الذي يلي الإفصاح. وسعت **دراسة(Berkman et al., 2018)**إلى محاولة تقديم مقياساً للوعي بالأمن السيبراني يعتمد على إفصاحات المنشآت للأمن السيبراني، من خلال **دراسة تطبيقة** على عينة من ٣٠٠٠ شركة أمريكية للفترة من ٢٠١٢إلى ٢٠١٦، **وتوصلت** إلى تطوير مقياس يلتقط مدى وأهمية عمليات الإفصاح وإظهار أن السوق يقدر بشكل إيجابي الوعي بالأمن السيبراني، وترتبط النغمة

السلبية في عمليات الإفصاح عن الأمن السيبراني بقيم السوق المنخفضة، وتوصلت إلى أن المنشآت التي تفصح عن قضايا الأمن السيبراني تحظى بتقدير أعلى من قبل السوق، وعلى الرغم من أن النبرة الإيجابية للإفصاح السيبراني لا تفسر القيمة السوقية.

في حين تمثل الهدف الرئيسي **لدراسة(الرشيدي، عباس، ٢٠١٩)** في التعرف على طبيعة الإفصاح عن المخاطر السيبرانية في التقارير المالية، وأثره على أسعار الأسهم وأحجام التداول في الشركات المصرية والأمريكية، وتم إجراء **دراسة مقارنة** عن طريق دراسة **الحدث** للشركات المصرية وشركتي (Facebook And Netflix)، **وخلصت النتائج** إلي ضعف الإفصاح عن المخاطر السيبرانية وإدارتها في الشركات المصرية مقارنة بالشركات الأمريكية، وما يحمله ذلك من آثار سلبية على أسعار الأسهم وأحجام التداول، ووجود تأثير جوهري للإفصاح عن المخاطر السيبرانية على أسعار الأسهم وزيادة أحجام التداول. واستكشفت **دراسة(McShane and Nguyen , 2020)**تأثيرات الأحداث السيبرانية على قيمة المنشأة ، واستخدمت **منهجية دراسة الحدث** لـ ٥٣٦ هجوم خلال الفترة ٢٠٠٧إلى ٢٠١٦، **وتوصلت** إلى أن شركات التجارة والتكنولوجيا أكثر تأثير سلبي في العوائد التراكمية غير الطبيعية، والمنشأة تتأثر سلباً للهجوم غير المباشر عن طريق الاستعانة بمصادر خارجية أكبر من الهجوم الداخلي، وتكبدت المنشآت بسبب هجمات التصيد الاحتيالي خسارة بنسبة٠,٥٤٪بينما أدت حوادث DOS إلى خسارة بنسبة ٠,٢٤٪، ووجود علاقة على شكل حرفU بين ردود فعل المساهمين للهجمات بمرور الوقت.

وركزت **دراسة(Tosun, 2021)**على تحليل كيفية استجابة الأسواق للإفصاح الالكتروني عن الهجمات السيبرانية في المنشآت الأمريكية في الأجلين القصير والطويل، وبلغت العينة الإجمالية ١١٨ شركة ضمن تسع قطاعات خلال الفترة من مارس ٢٠٠٤ إلى ديسمبر٢٠١٦، من خلال **دراسة تجريبية** ودراسة الحدث، **وأظهرت النتائج** أن العوائد التراكمية غير الطبيعية للأسهم تنخفض حيث تبلغ قوتها (-١,٤٪) في المتوسط يومياً ويزداد حجم التداول ويكون إيجابي، وتتأثر المنشآت بالإختراقات السيبرانية فقط في تاريخ الإعلان، وأن الإشارة السلبية على نسب مكاسب الأسعار التي تصل إلى خمس سنوات بعد خرق الأمان قد تشير إلى أن الإختراقات السيبرانية قد تؤثر جزئياً على قيمة المنشأة على المدى الطويل. في حين اهتمت **دراسة(Benaroch, 2021)**بالحوادث السيبرانية التي يسببها الطرف الثالث، وبيات تأثيراتها على القيمة السوقية للشركات، وبلغت العينة ١٣٩٧ حادث سيبراني بين عامي ٢٠٠٠ و ٢٠٢٠، منها ٢٤٦ حادثً تسبب بها طرف ثالث، من خلال منهجية دراسة الحدث **وتوصلت** إلى عدد من النتائج أهمها:(لا يتزايد انتشار الحوادث السيبرانية التي يسببها الطرف الثالث بشكل أسرع من الحوادث الأخرى، لكنها تعرض كميات أكبر من البيانات السرية لكل حادث، بالنسبة للتكاليف للحوادث التي يسببها الطرف الثالث، تعاني شركات العملاء (الطرف الأول) من انخفاضات في عوائد الأسهم.

وسعت **دراسة(حماده، ومهنى، ٢٠٢٢)**إلى اختبار العلاقة بين مستوى الإفصاح الإلكتروني للتقارير المالية و قيمة الشركة، واختبار العلاقة بين آليات الحوكمة و قيمة الشركة، بالإضافة إلى ذلك اختبار العلاقة التفاعلية بين آليات الحوكمة ومستوى الإفصاح الإلكتروني على قيمة الشركة، وذلك بالتطبيق على عينة من ١٢٣ شركة من الشركات المقيدة بالبورصة المصرية خلال عامي ٢٠١٨ ، ٢٠٢٠ تم استخدام نموذج الانحدار المتعدد لاختبار العلاقة بين متغيرات الدراسة، حيث تم قياس مستوى الإفصاح الإلكتروني للتقارير المالية لشركات العينة (متغير مستقل من خلال مؤشر خاص للإفصاح الإلكتروني يتكون من ٤٨ بنداً)، كما تم قياس آليات الحوكمة (متغير مستقل) من خلال ٦ آليات للحوكمة متمثلة في"استقلال أعضاء مجلس الإدارة، حجم مجلس الإدارة، ازدواجية دور المدير التنفيذي، الملكية الإدارية، الملكية المؤسسية، استقلال لجنة المراجعة"، كما تم قياس قيمة الشركة (متغير تابع) من خلال مؤشر(Tobin's Q)، وتم استخدام حجم الشركة والرفع المالي والربحية كمتغيرات ضابطة في نموذج الدراسة، وأظهرت النتائج وجود علاقة معنوية موجبة بين مستوى الإفصاح الإلكتروني و قيمة الشركة، كما أظهرت النتائج وجود علاقة معنوية بين حجم مجلس الإدارة و قيمة الشركة، أما باقى الآليات فقد أظهرت عدم وجود علاقة معنوية بينها وبين قيمة الشركة، أما عن العلاقة التفاعلية؛ فقد توصلت النتائج إلى عدم وجود تأثير لآليات الحوكمة على العلاقة بين مستوى الإفصاح الإلكتروني و قيمة الشركة، في حين جاءت النتائج توضح وجود علاقة موجبة بين حجم الشركة والرفع المالي و الربحية (المتغيرات الضابطة) وقيمة الشركة.

وارتكزت **دراسة(Masuch et al., 2022)**على فحص تأثير إجراءات الاستجابة لخرق البيانات على عوائد أسهم المنشآت المتضررة وتحليل ما إذا كان الإفصاح عن الإستجابة السريعة تخفف تلك العواقب، وتم استخدام منهجية **دراسة الحدث**، وتم اجراء **دراسة تطبيقية** على البيانات الثانوية تتعلق بـ ١٤١ حدث خلال عام ٢٠١١- ٢٠١٩، **وأظهرت النتائج** أن خروقات البيانات التي تتضمن بيانات العملاء تؤدي إلى ردود فعل سلبية في قيمة الأسهم، وعندما تفصح المنشأة عن الإستجابة السريعة لخرق البيانات، فإنه يؤثر بشكل إيجابي على قيمة الأسهم. في حين استهدفت **دراسة(Ali et al., 2022)**تقييم التأثير طويل المدى لانتهاكات تكنولوجيا المعلومات على مخاطر انهيار الأسهم، لـ ٢٧٦ انتهاكاً في المنشآت المتداولة من ٢٠٠٩ إلى ٢٠١٨، وأشارت النتائج إلى أن المنشآت المخالفة لديها مخاطر انهيار أسعار الأسهم أعلى بنسبة ٧٪ من المنشآت غير المخترقة، وأن الارتفاع في مخاطر انهيار أسعار الأسهم يكون أعلى إذا كان الانتهاك ينطوي على تنازل عن معلومات سرية وخرق متكرر لنفس المنشأة ، ويمكن أن يؤثر بشكل جوهري على القدرة التنافسية للمنشأة في المدى الطويل.

وفي هذا السياق، سعت **دراسة(يوسف، ٢٠٢٢)**إلى التعرف على واقع الإفصاح عن تقرير إدارة المخاطر السيبرانية، وأثره على أسعار الأسهم وأحجام التداول في المنشآت المصرية وعلى قرارات الاستثمار ومنح الائتمان، واستخدمت المنهج الوصفي وقائمة الاستقصاء، وقد **أظهرت** النتائج عدم إفصاح المنشآت المقيدة عن المخاطر السيبرانية وما يحمله من آثار سلبية على أسعار الأسهم وأحجام التداول، **وأوصت** بسرعة إصدار الإرشادات اللازمة لدعم الإفصاح عن أنشطة الأمن السيبراني، والحوادث تتعرض لها أو مخاطر تهددها وبرامج إدارة المخاطر السيبرانية، وأن يتولى مجلس معايير المحاسبة الدولية IASB إصدار معيار ينظم جوانب الإفصاح المحاسبي عن المخاطر السيبرانية وبرنامج إدارتها للشركات. **وأخيراً**، عملت دراسة**(Cao et al., 2023)**على تقييم استراتيجية الأمن السيبراني للشركات باستخدام التحليل النصي لتقارير(10-K)، ومستنداً على إطار الأمن السيبراني لـ(NIST, 2018)، وتم قياس خمس استراتيجيات مختلفة للأمن السيبراني، وهي:(تحديد الهوية والحماية والكشف والاستجابة والتعافي)سنوياً، وتكونت العينة النهائية بحساب درجات استراتيجية الأمن السيبراني لـ **٦٢٧٥٨ شركة** خلال الفترة ٢٠٠٥ إلى ٢٠١٨، **وتوصلت** إلى أن مناقشة استراتيجيات الأمن السيبراني في تقارير(10-K)(تحديد الهوية والكشف والاستجابة والتعافي)مرتبطة بشكل إيجابي وكبير بالقيمة السوقية للمنشأة (CARs) حول تاريخ إصدار التقرير، وتعد علامة على أن المنشأة تولي مزيداً من الاهتمام لاكتشاف الحوادث السيبرانية، وتجعل المستثمرين ينظرون إلى المنشأة التي تعرضت للهجوم بشكل أفضل، وإن الكشف عن استراتيجية حماية الأمن السيبراني لا يتم تقييمه بشكل إيجابي من قبل السوق، وتشير إلى أن المستثمرين يرون أن الإدارة فشلت في حماية المنشأة من الهجمات، وبالتالي تعاقب المنشأة على مناقشة استراتيجية الحماية في تقارير(10-K).

ومن استقراء وتحليل الدراسات السابقة يتضح للباحث أن الفجوة البحثية تتمثل فيما يلي :

- **بالنسبة للمجموعة الأولى(الإفصاح الالكتروني عن المخاطر السيبرانية):** فقد أكدت على أهمية الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها، وأن مخاطر فقدان البيانات السرية وتعطيل الخدمة هي مجالات رئيسية للمخاطر السيبرانية **(Gao et al., 2020)**، وأن الانتهاكات السيبرانية لها تأثير كبير على طول الإفصاحات**(Swift et al., 2020)**، وتوصلت دراسة **Chen et al., 2022)** أن المنشآت التي تعاني من خرق للبيانات تزيد من حجم إفصاحات عوامل المخاطر السيبرانية، ووجود علاقة إيجابية كبيرة بين استقلالية وخبرة مجلس الإدارة والإفصاح عن الأمن السيبراني**(Mazumder and Hossain, 2022)**. وتوصلت **دراسة(حماده، مهنى، ٢٠٢٢)**إلى وجود علاقة معنوية موجبة بين مستوى الإفصاح الإلكتروني و قيمة الشركة.**و**أوصت دراسة **(يعقوب وآخرون, ٢٠٢٢)** بضرورة تبني المؤشر المقترح للإفصاح عن المخاطر السيبرانية، **وأخيراً**، توصلت دراسة**(شرف، ٢٠٢٣)** إلى وجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين.
- **بالنسبة للمجموعة الثانية:(اهتمت بالعلاقة بين الإفصاح الالكتروني عن المخاطر السيبرانية وقيمة المنشأة):** وجود تباين في نتائج الدراسات السابقة؛ فقد توصلت بعض الدراسات إلى أن الهجمات السيبرانية لها تأثير سلبي ضعيف على القيمة السوقية للأسهم **(2019 ., Smith et al ; 2018 .,**

Amir et al)، على **عكس** دراستي **(Berkman et al., 2018; Barry et al., 2022)** التي توصلتا إلى أن المنشآت التي تفصح عن المزيد عن قضايا الأمن السيبراني تحظى بتقدير أعلى من قبل السوق، وتوصلت دراسة كل من**(الرشيدي، عباس، ٢٠١٩؛ Tosun, 2021)** إلى وجود تأثير سلبي وجوهري على أسعار الأسهم، وأكدت دراسة كل من**(McShane and Benaroch, 2021 ;Nguyen , 2020;** على أن المنشأة تتأثر سلبياً بشكل أكبر للهجوم غير المباشر عن طريق الاستعانة بمصادر خارجية، وتوصلت **دراسة (Ali et al., 2022)** إلى أن المنشآت المخالفة لديها مخاطر انهيار أسعار الأسهم أعلى بنسبة ٧٪ من المنشآت المنافسة غير المخترقة، **وأوصت دراسة(يوسف، ٢٠٢٢)**بسرعة إصدار معيار ينظم جوانب الإفصاح المحاسبي عن المخاطر السيبرانية وبرامج إدارتها للشركات، **وأخيراً، توصلت** دراسة**(Cao et al., 2023)** إلى أن مناقشة استراتيجيات الأمن السيبراني في تقارير(10-K)مرتبطة بشكل إيجابي بالقيمة السوقية، وتعد علامة على أن المنشأة تولي مزيداً من الاهتمام لاكتشاف الحوادث السيبرانية.

وتأسيساً على ما سبق، فإن الفجوة البحثية التي تثير التساؤلات المتعلقة بموضوع البحث، تتمثل الفجوة البحثية - في ضوء المسح الذي قام به الباحث- أنه لم تتطرق الدراسات السابقة لطبيعة وسياسات الإفصاح عن المخاطر السيبرانية وإدارتها على وجه التحديد في ضوء تكامل الأطر والتوجيهات والإرشادات المحاسبية للجهات والمجالس التنظيمة، وذلك بغرض إستخلاص إطار محاسبي مقترح للإفصاح عن المخاطر السيبرانية وبرامج إدارتها للإستجابة لمطالب أصحاب المصالح لتحقيق الإفصاح والشفافية في القوائم والتقارير السنوية، بحيث تعكس الأحداث الجوهرية للمنشأة، وتحليل تكاليف ومنافع الإفصاح عن هذه المخاطر وإنعكاساتها على قيمة المنشأة.

٤- **أهداف البحث:** يتمثل الهدف الرئيسي للبحث في عرض وتحليل الآثار الحالية والمحتملة للمخاطر السيبرانية في التقارير السنوية، وبيان محددات ومتطلبات الإفصاح عنها وإدارتها، وسيناريوهات مواجهتها وكيفية معالجتها والتخفيف من حدتها، في ضوء الأطر والإصدارات المحاسبية ذات الصلة، وتحديد أهم التحديات والمشاكل التي تعوق الإلتزام بها والتعرف على الآثار المترتبة عليها، فضلاً عن قياس أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها وكيفية معالجتها على مؤشرات على قيمة المنشأة.**<u>وينبثق من الهدف الرئيسي مجموعة الأهداف الفرعية التالية:</u>**

١- دراسة وتقييم مدى كفاية محتوى الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها وكيفية معالجتها في القطاعات المصرية محل الدراسة(البنوك- تكنولوجيا المعلومات والاتصالات).

٢- تحديد طبيعة واتجاه العلاقة بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة.

٣- قياس أثر الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها على القيمة السوقية في القطاعات المصرية محل الدراسة(البنوك- تكنولوجيا المعلومات والاتصالات).

٥- **أهمية البحث: تتمثل أهمية البحث فيما يلي:**

١/٥- الأهمية العلمية: تتمثل الأهمية العلمية للبحث فيما يلي:

١- إبراز الجوانب العلمية وتسليط الضوء على طبيعة المخاطر والتهديدات السيبرانية التي تتعرض لها منشآت الأعمال، والإفصاح عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها والمحددات والصعوبات التي تواجه تطبيق هذه الإفصاحات.

٢- تدعيم جهود البحث العلمى في مجال تعظيم قيمة المنشأة للشركات المصرية، والإسهام في تحقيق وتعزيز الميزة التنافسية وتحقيق وضع نظام معلومات مستقر ومحدث، يواكب التطورات في البيئة المحيطة نحو التحول للرقمنة، من خلال تعزيزممارسات الإفصاح الالكتروني عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها.

٣- يتطرق البحث إلي متغيرات حديثة في الجانب النظري والعملي والتحليلي، وبذلك يشكل البحث منطلقاً جديداً لمزيد من الدراسات اللاحقة حول هذا الموضوع.

٢/٥- الأهمية العملية: تتمثل الأهمية العملية للبحث فيما يلي:

١- تزايد أهمية الأمن السيبراني ومخاطره وتأثيراته الاقتصادية على أعمال المنشآت وأصولها، بسب التعرض للتهديدات والحوادث السيبرانية، والتي أفقدت المنشأت أموال طائلة وأثرت على أدائها، وسمعتها.

٢- إرساء الضوابط والأطر المنهجية في مجال الأمن السيبراني في ضوء سعي المنشآت بشكل مستمر إلى مراقبة تقارير الإفصاح لتجنب المخاطر السيبرانية، وتحديد الأولويات وتنظيم المعلومات حول المخاطر الفعلية والمحتملة التي تهم جميع الأطراف.

٣- محاولة تفعيل وربط الجهود الأكاديمية بالخطوات التنفيذية في الواقع العملي وذلك بتطبيق المؤشر المقترح في المنشآت محل الدراسة لتهيئة ومساعدة المسئولين للقيام بأدوارهم في تعزيز وتحسين رقابة وإدارة المخاطر السيبرانية، كما أن شكل ومضمون الإفصاح عن هذه المخاطر من الممكن أن تحسن الشفافية وتفيد اصحاب المصالح في اتخاذ القرارات.

٦- فروض البحث:

في ضوء تساؤلات البحث وسعياً نحو تحقيق أهدافه، واستناداً على استقراء وتحليل الدراسات السابقة المتعلقة بمتغيراته، يمكن صياغة فروض البحث على النحو التالي:

١- يوجد تفاوت في الإفصاح الإلكتروني عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.

٢- يوجد ارتباط معنوي بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة.

٣- يوجد أثر ذو دلالة إحصائية للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة.

٧- منهجية البحث:

اعتمد البحث على **المنهج الإستنباطي**، ويستهدف الباحث من خلال هذا المنهج إجراء الاطار النظرى للبحث؛ وذلك بالإطلاع على الدراسات السابقة والبحوث بالمجلات العلمية والنشرات الدورية والسلاسل الزمنية للجهاز القومي للإتصالات والبورصة المصرية، والضوابط والأطر والإرشادات الرقابية والإصدارات المهنية لممارسات المنشآت في الإفصاح الالكتروني عن المخاطر السيبرانية وإدارتها، وكيفية معالجتها والتخفيف من حدتها، **والمنهج الاستقرائى**، وسيعتمد الباحث علي هذا المنهج في إجراء الدراسة التطبيقية علي عينة من المنشآت المصرية المقيدة بالبورصة المصرية، وذلك لدراسة وتحليل أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها وكيفية معالجتها بالتقارير السنوية والإيضاحات المتممة لأصحاب المصالح علي مؤشرات قياس قيمة المنشأة.

٨- **حدود البحث:** ستقتصر الدراسة علي:

- **حدود مكانية:** تقتصر الدراسة التطبيقية علي المنشآت المصرية المقيدة بالبورصة المصرية ضمن قطاعي(البنوك- تكنولوجيا المعلومات والاتصالات والإعلام)، وذلك نظراً لتوافر القوائم والتقارير السنوية المنشورة لتسهيل جمع وتحليل البيانات اللازمة لتحقيق أهداف الدراسة واختبار فروضها.
- **حدود زمنية:** تم اختيار سلسلة زمنية قدرها ٣ سنوات تبدأ من عام ٢٠١٩ وتنتهي بعام ٢٠٢١.

٩- **خطة البحث:** في ضوء مشكلة البحث، وسعياً نحو تحقيق أهدافه، وتجسيداً لاختبار فروضه، واعتماداً على منهجه، لاستخلاص أهم النتائج والتوصيات، تم تقسيم هذا البحث، على هذا النحو التالي:

أولاً: الإطار العام للبحث.

ثانياً: المخاطر السيبرانية بين المفهوم و الآثار المحتملة والقياس الكمي

ثالثاً: دراسة تحليلية لمتطلبات الإفصاح الالكتروني عن المخاطر السيبرانية وإدارتها في ضوء الأطر والإرشادات التنظيمية.

رابعاً: جهود المؤسسات التنظيمية والرقابية للفكر المحاسبي في الإفصاح الالكتروني عن المخاطر السيبرانية.

خامساً: قيمة المنشأة من منظور محاسبي(بين المفهوم ومداخل القياس).

سادساً: الدراسة التطبيقية واختبارات الفروض.
سابعاً: النتائج والتوصيات والدراسات المستقبلية.
وفيما يلي عرض تفصيلي لباقي محاور خطة البحث.

ثانياً: المخاطر السيبرانية بين المفهوم و الآثار المحتملة والقياس الكمي

١/٢- ماهية وأنواع المخاطر السيبرانية.

ليس من السهل تحديد تعريف للمخاطر السيبرانية، حيث إن البحث العلمي في هذا الصدد لم يعتمد بعد معياراً، وإنها في الواقع فئة معقدة من المخاطر(MIele, 2022, p1). ويمكن النظر إلى المخاطر التي تواجهها المنشآت في بيئة من الهجمات السيبرانية من ثلاثة جوانب، تتمثل في:(تحديد وتجميع التهديدات السيبرانية، واتخاذ تدابير لتقليلها أو القضاء عليها، وبناء نظام مناسب لحماية المعلومات المحاسبية)(Mironchuk and Maletska, 2022, p154). وتم تحديد الأمن السيبراني في مجال نظم المعلومات المحاسبية AIS للتركيز على منع الضرر والاستخدام غير المصرح به واستغلال المعلومات والنظم المحاسبية، وكذلك ضمان هذه الأنظمة وحوكمتها واستعادتها، من أجل تعزيز السرية والنزاهة والتوافر(Cram et al., 2022, p6). ويعكس الأمن السيبراني عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، ويحتوي على طبقات متعددة من الحماية تنتشر عبر أجهزة الحاسب الآلي أو الشبكات أو البرامج لإنشاء دفاع فعال في مواجهة الهجمات السيبرانية(شحاته والبردان، ٢٠٢١، ص٩).

ويشير(Strupczewski, 2021, p6) إلى عدم وجود توافق في الآراء بشأن المعنى الدقيق للمخاطر السيبرانية، وعرفها بأنها مخاطر تشغيلية مرتبطة بأداء الأنشطة في الفضاء السيبراني، والتي تهدد أصول المعلومات والأصول التكنولوجية، والتي قد تسبب ضرراً مادياً للأصول الملموسة وغير الملموسة. وتشمل التهديدات المادية لإعادة مصادر تكنولوجيا المعلومات والاتصالات داخل المنشأة (Heidenborg and Lappalainen, 2021, p2). وتنطوي المخاطر السيبرانية على حدث إلكتروني ضار يسبب في تعطل الأعمال التجارية والخسارة النقدية (Pacheco-Paredes and Wheatley, 2022, p2, 6). وفي إطار عمل **لجنة بازل الثالثة**، تعد المخاطر السيبرانية فئة فرعية من المخاطر التشغيلية، وأدخلت اللجنة نظام تصنيف يتضمن الحوادث السيبرانية، مما يثبت الترابط المفاهيمي بين المخاطر التشغيلية والسيبرانية (Curti et al., 2022, p4). وهي شكل من أشكال المخاطر التشغيلية المتعلقة بشكل أساسي بتكبد الخسائر الناتجة عن الحوادث الرقمية التي تسببها أطراف داخلية أو خارجية، بما في ذلك السرقة والإخلال بالنزاهة والإضرار بمصادر المعلومات والتكنولوجيا والاحتيال (Ferens, 2021, p36). وأشارت دراسة(الفقي، ٢٠٢١، ص١٧)بأنها المخاطر التي تنشأ عندما يقدم البنك منتج جديد أو خدمة أو عملية تجارية أو نشاطاً داعماً أو أصلا رقمياً أو يعتمد على التكنولوجيا الرقمية. وباتجاه آخر، فقد عرفتها(الهيئة المصرية للأمن السيبراني المصري، ٢٠١٨، ١١٩) بأنها المخاطر التي يمكن أن تواجه المنشآت بما فيها رسالة المنشأة ورؤيتها أو شعارها أو سمعتها، بسبب إمكانية الوصول غير المصرح أو سوء الاستخدام أو تدمير المعلومات. ووصفتها دراسة (Varga et al., 2021, p9)بأنها مخاطر تشغيلية غير مالية في الأصل بغض النظر عن المنشأ، وهذه المخاطر تنطوي على تكاليف. وقد أكدت دراسة كل من (Hartmann and Carmenate, 2021; Florackis et al., 2023, p352)على أنها مخاطر الخسارة المالية أو الانقطاع التشغيلي أو الإضرار بسمعة المنشأة نتيجة الفشل في أنظمة تكنولوجيا المعلومات الرقمية.

وفي ظل السعي لوضع تعريف وصياغة مفهوم للمخاطر السيبرانية، يري الباحث أنها عبارة عن مدى تعرض الوحدة الاقتصادية لخسائر(مالية وغير مالية)واسعة النطاق، وغير متوقعة ونتائج غير مرغوب فيها، نتيجة حدوث تهديدات محتملة غير مؤكدة للإضرار بسرية ونزاهة وتوافر البيانات والمعلومات الخاصة في الفضاء السيبراني، مما يؤثر على قدرتها على تحقيق أهدافها واستمراريتها في حالة وقوع هذه المخاطر.

وباستقراء الفكر المحاسبي؛ فيما يتعلق بتصنيف المخاطر السيبرانية التي تواجهها المنشآت، لا تتعرض كل الصناعات بشكل متطابق للمخاطر السيبرانية. ويتوقف ذلك على عدة عوامل مثل طبيعة المخاطر

وإمكانية حدوث خسائر، حيث تباينت الآراء حول التصنيفات المختلفة للمخاطر السيبرانية في القطاعات كالتالي:(نشرة الاتحاد المصري للتأمين ،٢٠١٩، ٣-١٧؛ يعقوب وآخرون, ٢٠٢٢، ص١٤١٤، جبر، ٢٠٢٢، ص ٩):**(سرقة أو فقدان البيانات،** البيانات الشخصية والبيانات التجارية، وأي بيانات ذات قيمة بالسوق تعتبر خطر، والدافع هو البحث عن المكاسب المالية أو التنافسية، و**تدمير البيانات،** مسح البيانات السيبرانية أو تشفيرها أو منع الوصول إليها، والدافع هو الابتزاز، و**انقطاع الاتصالات،** تعطيل الموقع الالكتروني أو تعطيل الشبكة؛ تشويه الموقع للاستيلاء على صفحات وسائل التواصل الاجتماعي والدافع هو الابتزاز، والإرهاب، أو التجسس. **كما اتفقت دراستي**(شحاته والبردان،٢٠٢١، ص١٠-١١؛ السواح، ٢٠٢١، ص٥٠٦-٥١١) على تصنيف المخاطر السيبرانية إلى **ثلاث أنواع** من المخاطر على النحو التالي:(**المخاطر المتعلقة بتأمين البيانات والمعلومات:** وهي المخاطر الناشئة من تخرين البيانات والمعلومات للأفراد والمؤسسات ومن الممكن تعرضها إلى الاختراق، أو نقلها للمنافسين، **والمخاطر المتعلقة بانتهاك الخصوصية:** وهي المخاطر الناتجة عن مخاطر سرقة البيانات الشخصية، و**المخاطر المتعلقة بانتهاك حقوق الملكية الفكرية:** وتتمثل في المخاطر المتعلقة بحقوق الملكية الفكرية والأدبية نتيجة نسخ الوسائط الرقمية وإعادة إنتاجها وتأخر مستوى التشريعات القانونية).

وفيما يلي الأساليب الشائعة الاستخدام في أنواع الهجمات السيبرانية (الأمير، ٢٠٢٢، ص٤٩٦-٤٩٧؛ Shahid and Hau Huang, 2020, p14; Hasan and Al-Ramadan, 2021, p2313-2315; Axelrod, 2022, p3-4; Doerr et al., 2022, p4-5; Serkan and Ahmet, 2022, p716; Vlčko and Meluchová, 2022, p78;Haruna et al., 2022, p1-3; Sukumar et al., 2023, p3,5):**احتيال المعلومات والبيانات،** وهو التعديل غير المصرح به للبيانات قبل أو أثناء تسجيل الدخول إلى نظام الكمبيوتر واستعادتها بعد اكتمال العملية، **والقرصنة،** وتسمى الوصول غير المصرح به إلى أنظمة الكمبيوتر، **وانتشار الفيروسات،** ويتم إضافة برامج ضارة إلى نظام آخر بغرض تدمير النظام المهاجم، **والقنبلة المنطقية،** وتعمل هذه البرامج الضارة بشكل مشابه للقنبلة الموقوتة، **ورفض الخدمات (DoS)** وتستنزف هذه الهجمات موارد النظام، وتطغى عليها، وتمنعه من الاستجابة لطلبات الخدمة، مما يقلل بشكل كبير من قدرة النظام على الأداء، والغرض من هجمات DoS هو عادةً إنشاء رفض للخدمة أو هجوم ثانوي مختلف، **والتصيد الاحتيالي** لاستخراج معلومات سرية مثل أرقام بطاقات الائتمان ومجموعات اسم المستخدم وكلمة المرور من خلال التظاهر بأنها منظمة شرعية، **وهجمات الدودة وأحصنة طروادة.**

ويصنف **مجلس التقارير المالية(FRC)** مخاطر الأمن الرقمي إلى(FRC, 2022, p3):(**مخاطر الأمن الرقمي،** وهي المخاطر التشغيلية والمالية والمتعلقة بالسمعة وأصحاب المصلحة الناتجة عن تهديدات الأمن السيبراني، بما في ذلك مخاطر الانتهاكات الكبيرة للبيانات الناشئة عن الثغرات الداخلية، و**مخاطر الاستراتيجية الرقمية:** هي المخاطر التشغيلية والمالية والسمعة وأصحاب المصلحة الناتجة عن الانتقال إلى نموذج الأعمال الرقمية (يشار إليه أيضاً بالتحول الرقمي) وزيادة الاعتماد على البيانات. وقامت لجنة التكنولوجيا في **الاتحاد الدولي للمحاسبين IFAC** بتصنيفها إلي **ثلاث** أنواع هي:(مخاطر البنية التحتية لنظم تكنولوجيا المعلومات- مخاطر تطبيق تكنولوجيا المعلومات- مخاطر تكنولوجيا المعلومات الخاصة بأعمال المنشأة)(السواح، ٢٠٢١، ص٤٩٤). ووفقاً لتقرير(PwC, 2022) تعرضت واحدة من كل أربع شركات(٢٧٪)على مستوى العالم لخرق في البيانات كلفها ما بين ١ و ٢٠ مليون دولار أو أكثر في السنوات الثلاث الماضية، وترتفع النسبة إلى واحد من كل ثلاثة(٣٤٪)للشركات في أمريكا الشمالية، حيث أبلغت ١٤٪ فقط من المنشآت على مستوى العالم عن عدم حدوث انتهاكات للبيانات خلال هذه الفترة.

٢/٢- تحليل الآثار المحتملة للمخاطر السيبرانية على النظام المحاسبي

نظراً لأن المحاسبة هي المولد الرئيسي للمعلومات الاقتصادية، فإن المعلومات المحاسبية تتطلب الأمن السيبراني في المقام الأول، ويتم تحديد الفئات الرئيسية للتهديدات التي تتعرض لها المعلومات المحاسبية على أنها نشطة وسلبية(Igor, et al., 2022, p966). وترتبط المخاطر السيبرانية بسرقة المعلومات المحاسبية أو تقليل معايير الجودة الخاصة بها، ويتم ضمان الأمن الاقتصادي للمؤسسة من خلال الامتثال للخصائص النوعية للمعلومات المحاسبية، وقد يؤدي انتهاك أي من معايير الجودة للنظام المحاسبي إلى فقدان فائدته، وبالتالي أهميته الاقتصادية للمستخدمين(Zadorozhnyi et al., 2021, p36).

ويتطلب تفعيل المخاطر السيبرانية المتغيرة في المحاسبة تطوير وسائل معيارية فعالة للقضاء عليها، لضمان الأمن السيبراني(الحماية السيبرانية) للمعلومات المحاسبية، ولقد ثبت أن جودة المعلومات المحاسبية وموثوقيتها، هي أولوية في تطوير أحدث تقنيات الكمبيوتر والاتصالات وظهور التهديدات السيبراني، ويجب وضع موثوقية البيانات المحاسبية على أنها عدم وجود أخطاء أو تشوهات، ويتم تحديد قائمة المبادئ الأساسية للحماية السيبرانية للمعلومات المحاسبية، والتي تشمل السرية والنزاهة والتوافر والاكتمال وامكانية الوصول والموثوقية والقابلية للمقارنة، ومبادئ الأمن السيبراني هي الأساس لتطوير التعليمات المنهجية للحماية السيبرانية للشركات، لمنع وتجنب والقضاء على عواقب التهديدات لأمن وجودة المعلومات المحاسبية(Muravskyi et al., 2022, p103). ولا يستطيع العديد من المحاسبين التعامل مع التطورات السريعة لتكنولوجيا المعلومات والتعرض للجرائم السيبرانية (Boban et al., 2018,p541). وعندما تعاني المنشآت من أوجه قصور في الرقابة الداخلية على تكنولوجيا المعلومات، فمن المحتمل أن تكون أوجه القصور هذه مرتبطة بمخاطر وانتهاكات الأمن السيبراني، وبموجب المادة ٤٠٤ من قانون(SOX) يجب على المراجعين التصديق على الرقابة الداخلية على التقارير المالية (ICFR) والإبلاغ عند اكتشاف أي ضعف في الرقابة الداخلية (ICW) من قبل المراجعين (Cheong et al., 2021,p180).

٣/٢- طبيعة وكيفية القياس الكمي للمخاطر السيبرانية

يقصد **بالقياس الكمي للمخاطر السيبرانية** بأنه عملية تقييم المخاطر السيبرانية التي تم تحديدها ثم التحقق من صحة البيانات السيبرانية المتاحة وتحليلها، والقيمة المعرضة للخطر (VaR) التي تمت مناقشتها في اجتماع المنتدى الاقتصادي العالمي في ٢٠١٥، وتمت دراسة القيمة المعرضة للمخاطر وبحثها واعتبرت طريقة قابلة للتطبيق لقياس المخاطر السيبرانية(Ghosh, 2020, p2).

ويعد القياس الكمي للضرر الناجم عن الهجمات السيبرانية أحد أكثر الجوانب صعوبة في تحديد حجم التأثير، وأن الضرر يظهر من خلال **أربع آليات**: (١) انخفاض الحصة السوقية؛ (٢) انخفاض سعر السهم؛ (٣) زيادة تكلفة رأس المال؛ (٤) زيادة تكلفة الحصول على الموظفين والاحتفاظ بهم(Pollmeier et al., 2023, p4).

١/٣/٢- القياس الكمي للمخاطر السيبرانية من خلال إطار الاستجابة للحواث.

أصبح مطلب إنشاء منصة استخبارات للتهديدات السيبرانية داخل المنشأة ضرورة ملحة للعديد من المنشآت، وتسهل منصة استخبارات التهديدات السيبرانية منع الحوادث وآلية الإبلاغ الرسمية والاستجابة للحوادث، وفي هذه العملية يتم تحديد كل من التهديد والضعف كمقاييس مهمة في تقييم المخاطر السيبرانية، ويتم حساب المخاطر في الأمن السيبراني من خلال المعادلة التالية Ghosh, 2020, p5; Sharma and Mukhopadhya, 2022, p3; Sukumar et al., 2023, p4):

المخاطر= التهديد x الضعف x الأصول

ويبدأ مفهوم **إطار الاستجابة** للمخاطر بتحديد عوامل الخطر في إطار الفئات الثلاث على النحو التالي:(تحديد التهديدات وترتيب أولوياتها، وتحديد مواطن الضعف وتحديد أولوياتها، وتحديد الأصول وترتيب أولوياتها)(Ghosh, 2020, p1). وتشمل **أطرالاستجابة** وضع قائمة بالإجراءات المتخذة مثل(خطوات التصعيد، وأنشطة الاستجابة والتعافي، وإبلاغ أصحاب المصلحة)، وتحديد الإجراءات لتنفيذ التدابير لضمان عدم تكرار حوادث مماثلة(Cao et al., 2023, p6081; Doerr et al., 2022, p4). ويتم إثبات **مرحلة التحديد** من خلال تحديد كمية المخاطر، ويتوخى تقييم المخاطر المتعلقة بالتهديدات ومواطن الضعف مع تقييم الأصول من أجل عملية مثالية للتقدير الكمي، وتحديد حجم الحوادث المكتشفة والاستجابة لها(CBB, 2021, p6). ويعد **تحديد الأصول** الهامة(مثل البيانات والأجهزة والتطبيقات والشبكات)أمراً إلزامياً لفهم المخاطر السيبرانية للمنشأة، ويعتمد التأثير على البيانات المحتملة المتأثرة مثل(بيانات PHI، والملكية الفكرية)، والأجهزة المتأثرة(مواقع الويب، والآلات، والأجهزة)، والتطبيقات المتأثرة(مثل الخدمات الرئيسية، والبرامج)، والمستخدمون المتأثرون، واستنزاف الموارد بشكل عام على المنشأة(Leirvik, 2022, p41). ويتمثل النشاط الأكثر أهمية في إجراء تقييم المخاطر السيبرانية؛ في تحديد الأصول الرقمية الأكثر قيمة للمؤسسة وتحديد ما يمكن أن يعنيه إذا تم اختراقها، وليس من السهل

تحديد حجم الخسارة، خاصةً إذا لم يكن للأصول قيمة محاسبية (مثل السجلات الإدارية وبيانات العميل والملكية الفكرية)(عثمان، ٢٠٢٢، ص٧).

ويصبح من مسؤولية مدير المخاطر تحديد الأصول التي تريد المنظمة حمايتها، وإن الطبيعة المترابطة لمجموعات الأمن السيبراني تجعل هذه المهمة صعبة، ويعد **تحديد الأصول** محل الاهتمام أمراً بالغ الأهمية لتطوير إطار عمل مناسب لإدارة المخاطر الإلكترونية، وغالباً ما تكون هناك أصول متعددة متضمنة في سيناريو واحد، وإن فهم نوع التهديد مهم بنفس القدر لأنه يقود عدد تحليلات السيناريوهات المطلوبة، يتم **تصنيف سيناريوهات الأمن السيبراني** عموماً إلى **ثلاث** مجموعات، بناءً على التأثير الذي يمكن أن تحدثه على الأصول الرقمية: (السرية والنزاهة والتوافر)، وفي كثير من الأحيان، قد تبدو السيناريوهات متداخلة بين مجموعتين أو حتى كل المجموعات الثلاث، وفي هذه الحالة، يجب أن يكون التركيز والتصنيف الأساسيان على الأثر الأكثر صلة، والذي من المحتمل أن يؤدي إلى خسائر للشركة(Pollmeier et al., 2023, p3).

وتدعم المعايير الدولية للتقرير المالي منهجية كمية لتقدير التأثير على الأصول المعرضة للمخاطر، وكميزة إلزامية تشترط**(IFRS)**إعادة تقييم الأصول باستخدام القيمة العادلة، وبالتالي، فإن الصلة بين البيانات المالية وإدارة المخاطر المتعلقة بالأمن السيبراني، تكمن في العلاقة بين القيمة العادلة والتدهور الناتج ومخاطر الأصول التكنولوجية(Moncayo and Montenegro, 2019, p115). ويجب تطوير خطة تحمل المخاطر السيبرانية من خلال النظر في التأثيرات المختلفة للتهديدات السيبرانية بما في ذلك تعطل الخدمة، والخسارة المالية، وإدارة الأصول (الأجهزة والبرامج)، وإدارة الحوادث(الإفصاح والاستجابة)، وإدارة مخاطر الطرف الثالث، والمرونة السيبرانية (استمرارية الأعمال والتخطيط لمواجهة الكوارث) (CBB, 2021, p6). **ومن وجهة النظر الكمية**، يمكن الاتفاق مع المعايير الدولية للإبلاغ المالي، بإمكانية إعادة تقييم أصول تكنولوجيا المعلومات والاتصالات كل سنة، وفقاً للسياسات المحاسبية التي تحددها المنشأة؛ وعندما يكون هناك تدهور، قد يكون الأصل ضعيفاً لأن النمو التكنولوجي يمكن أن يكون له آثار سلبية على الوضع العادي لتشغيله، على سبيل المثال، نقص الدعم الفني، وقد تكون للأصول قيمة عادلة في والتقادم التكنولوجي ليس نقطة ضعف؛ ومع ذلك، فمن المهم تحليل أنواع الثغرات الأمنية الأخرى، على سبيل المثال، المخاطر الأمنية والأمن المادي ,Moncayo and Montenegro, 2019) (p116. ويجب تحديد **الأصول الملموسة** المشاركة في إدارة المخاطر من الناحية الكمية، بناءً على القيمة الدفترية والقيمة العادلة واستهلاك مكونات الأجهزة (Hw)، **والأصول غير الملموسة** هي الخدمات(S) والبرامج (Sw) والأشخاص (P) ودعم المعلومات (IS)؛ يتم تحديدها من مستنداتها القانونية والتكنولوجية (العقود، التراخيص، العمليات، إلخ)، ومن ناحية أخرى، إذا كان التأثير يركز على التكلفة، فيجب أن يكون التقدير كمياً؛ في هذه الحالة، إذا كانت القيمة الدفترية للأصل(BV)أكبر من قيمتها العادلة(FV)، فإن الفرق سيؤدي إلى خسارة أو تدهور(Moncayo and Montenegro, 2019, p117).

٢/٣/٢- قياس المخاطر السيبرانية وفقاً التكاليف التشغيلية:

تحلل العديد من الدراسات مثل Paul and Wang, 2019; Uddin et al., 2020; Manoj, 2021; Sharif and Mohammed, 2022). كيف يمكن للمخاطر السيبرانية أن تزيد من التكاليف التشغيلية، ولا يمكن التخفيف من المخاطر السيبرانية فقط من خلال التطوير للبنية التحتية لتكنولوجيا المعلومات، لأنه يزيد من التكاليف التشغيلية ولكن لا يمكن أن تضمن وقف الانتهاكات السيبرانية، حيث يحتاج الاستثمار في الغالب إلى مجالات مثل الحصول على الأجهزة والبرامج الأكثر موثوقية، وأنظمة تشفير البيانات، وجدران الحماية، والمراقبة السيبرانية، وأنظمة الإفصاح عن المخاطر. كما ذكرت(SEC ,2018: 3–4) أن تكلفة الهجمات السيبرانية تشمل "تكاليف الإصلاح مثل المسؤولية عن الأصول أو المعلومات المسروقة، وإصلاح تلف النظام، وزيادة تكاليف حماية الأمن السيبراني والتي قد تشمل تكاليف إجراء تغييرات تنظيمية، والتقاضي، بما في ذلك الإجراءات التنظيمية؛ وزيادة أقساط التأمين؛ الإضرار بالسمعة Héroux and Fortin, 2020, p79; Gatzert and Schubert, 2022, (p727).

وتشمل التكاليف المتعلقة بالأصول والأنشطة التي تنطوي عليها عمليات المنشأة ، والمنطقة المسؤولة عن دعم السلع أو تقديم الخدمات، وتكلفة التدهور، والعطل، وإساءة الاستخدام، وعدم التوافر، واسترداد الأصول، والبرامج وأجهزة تكنولوجيا المعلومات والمستندات والمعدات والأنشطة، ويمكن تمثيل هذه التأثيرات بخصائص مالية، كالتالي:(**التدهور- الأعطال- إساءة الاستخدام- عدم توفر الأصل أو النشاط- الاسترداد)**(Couce-Vieira et al., 2020) . ويمكن تكوين **احتياطي (مخصص)**ما بعد الخسارة، وهو صندوق الطوارئ يتم إنشاؤه لتغطية الخسائر الناتجة عن الحوادث السيبرانية، مثل تكاليف الطب الشرعي، وتكاليف إصلاح أو استبدال الأصول السيبرانية، والالتزامات القانونية في حالة الدعاوى القضائية، أن هذا الصندوق محجوز بالفعل قبل وقوع أي حوادث إلكترونية، ولكن يتم استخدامه بعد ذلك لاستيعاب وامتصاص الخسائر بعد الحوادث، وهو ما يفسر تأثيره بعد الخسارة(Chong et al., 2022).

ويمكن تصنيف تكاليف الاختراقات السيبرانية إلى **مجموعتين** من حيث **الفترة المحاسبية**، كالتالي: **المجموعة الأولى:** (تكاليف مؤقتة- قصيرة الأجل)، وهي التي يتم تحملها فقط خلال الفترة التي حدث فيها الإختراق، وتشمل خسارة الأعمال، وانخفاض الإنتاجية نتيجة عدم توفر الموارد، وتكاليف الإصلاح للموارد المخترقة، وتكاليف جمع الأدلة عن القائم بالإختراق، **والمجموعة الثانية:** (تكاليف دائمة -طويلة الأجل) وهي التي تؤثر على عدة فترات محاسبية، وهي ترتبط بضياع التدفقات النقدية المستقبلية للمنشأة ، وفقد العملاء وتحولهم إلى المنافسين، وعدم القدرة على جذب عملاء جدد بسبب ضعف المنظومة الأمنية السيبرانية، وفقد ثقة المستثمرين، وزيادة تكلفة رأس المال(فرج, ٢٠٢٢).

٣/٣/٢- قياس المخاطر السيبرانية وفقاً للقيمة السيبرانية المعرضة للخطر:

بالنسبة لهذه المخاطر، فإن قياس المخاطر السيبرانية مالياً يتضمن **عنصرين: تكرار حدث الخسارة وحجم الخسارة**(Strupczewski, 2021). وأحد أبرز النماذج هو تحليل العوامل لمخاطر المعلومات (FAIR)، والذي يوجه خبراء الأمن السيبراني في تحليل عناصر المخاطر السيبرانية إلى أجزاء قابلة للقياس الكمي، وإن تكرار حدث الخسارة مدفوع بتكرار الاتصال، واحتمال حدوث الفعل، والقدرة على التهديد، والصعوبة، وينقسم حجم الخسارة إلى خسارة أولية وخسارة ثانوية، ثم يتم استخدام تقدير الخبراء بالاقتران مع الأدوات الإحصائية لتقييم الأثر المالي للمخاطر السيبرانية، ويتمثل العائق الطبيعي لتطوير هذه النماذج الكمية، في ما إذا كانت الشركة لديها البيانات المتاحة لإنشاء تقديرات لتكرار حدث الخسارة وحجمها، خاصةً إذا كانت تعتمد تاريخياً على أطر نوعية قائمة على الامتثال، ويتضمن قياس حجم المخاطر في جوهره ببساطة تطبيق تقديرات مُعايرة لسيناريوهات المخاطر المحددة، والاعتماد على تقديرات من الداخل(أو الخبراء) هو عنصر أساسي في النماذج الكمية، ويدعو المنهج الكمي إلى استخدام قدرات احتمالية صريحة، معبر عنها خلال فترة زمنية والخسائر المتوقعة معبراً عنها في صورة فترة ثقة، ويمكن استخدامها لتوليد منحنى تجاوز الخسارة الذي يمكن أن يوفر للمديرين رؤى أكثر دقة وفائدة من مصفوفة المخاطر التقليدية(Pollmeier et al., 2023, p3).

وتمت صياغة أول اقتراح لتطبيق مقياس تقليدي للمخاطر المالية مثل القيمة المعرضة للمخاطر في مجال الأمن السيبراني في عام ٢٠١٥، كجزء من مبادرة المرونة السيبرانية التي يرعاها المنتدى الاقتصادي العالمي، والتي أدت إلى ظهور الإطار المفاهيمي للقيمة السيبرانية المعرضة للخطر(Cy-VaR)(Eling and Wirfs, 2019, p1114). عرفت **لجنة بازل** القيمة المعرضة للخطر"ما هو الحد الأقصى للخسارة التي يمكن تكبدها في فترة زمنية معينة، بحيث يكون هناك احتمال ضئيل للغاية بأن الخسارة الفعلية ستكون أكبر من القيمة المقدرة؟"(BCBS, 2018). ومن هذا السؤال يمكن استنتاج العنصرين الرئيسيين المشتركين في جميع النماذج التي تنتمي إلى عائلة القيمة المعرضة للمخاطر، وهما(MIele, 2022, p16):

١- **وجود مدى زمني ثابت**، وهي عبارة عن الوحدة الزمنية المستخدمة في قياس المخاطر، والذي يمكن أن يكون قصيراً إلى حد ما بالنسبة لنوع المخاطر التي ينطوي عليها الأمر؛ على سبيل المثال، سيتطلب تقييم مخاطر السوق بالتأكيد مدى زمنياً قصيراً جداً، عادةً يومياً أو أسبوعياً، في حين يمكن تقييم المخاطر التشغيلية على مدى فترة أطول، عادةً ما تكون سنوية.

٢- **مستوى ثقة محدد مسبقاً**، أي الاحتمالية التي نتأكد من خلالها أن تقدير القيمة المعرضة للمخاطر لن تتجاوزه الخسارة الفعلية، وبطبيعة الحال، فإن اختيار مستوى أعلى من الثقة سيؤدي أيضا إلى تقدير أعلى للقيمة المعرضة للخطر؛ بشكل نموذجي، وعادةً، يتم تقدير var عند مستوى الثقة ٩٥ أو ٩٧,٥ أو ٩٩ بالمائة، ويعني تحديد مستوى ثقة بنسبة ٩٩٪ أنه سيتم تجاوز التقدير الذي تم إجراؤه باحتمال ١٪ فقط. ويتراوح مستوي الثقة في الدراسات الاجتماعية والمالية بين ٩٠% و ٩٩% ويعبر عن درجة الثقة في نتائج قياس النموذج للمخاطر(الامبابي, ٢٠٢٢، صـ٥٨٧).

وعلى الرغم من أنه لا يوفر نهجاً تشغيلياً موحداً حقيقياً لتقدير المخاطر السيبرانية، إلا أن المقترح يحتوي على مؤشرات قيمة، لبناء طريقة شاملة وموحدة لمختلف القطاعات الإقتصادية، مما يشجع المنشآت على بناء النماذج الخاصة بها للتقدير الكمي الداخلي، وبالتالي فإن Cy-VaR يفسح المجال لأن يكون مؤشراً بديلاً للتعرض للمخاطر السيبرانية أكثر من كونه تقديراً دقيقاً لها؛ ومع ذلك ، فإن التوحيد القياسي عبر مختلف قطاعات الاقتصاد لمثل هذا المؤشر سيزيد بالتأكيد من فائدته(MIele, 2022, p18).

وبالتالي، فإن Cy-VaR هو مقياس محاسبي يمكن استخدامه كمكمل للتقييمات الفنية اللازمة على مستوى أمن تكنولوجيا المعلومات للمنشأة (Eling, and Jung, 2022, 4). والذي يساعد أيضاً من خلال قياس الأثر الاقتصادي للهجمات السيبرانية على توجيه خيارات المديرين فيما يتعلق بالاستثمارات في الأمن السيبراني وتخفيف المخاطر(على سبيل المثال، شراء بوليصة تأمين) أو لتقدير الحد من التعرض الناتج عن هذه الخيارات(Curti et al., 2019, p7). وأوردت دراسة (Orlando, 2021) مثال عملي على هذا النوع من التطبيقات، والذي اقترح عائداً معدلاً حسب المخاطر على مؤشر الاستثمار الأمني يسمى RaROSI39 (العائد المعدل حسب المخاطر على الاستثمارات الأمنية) ويتم بناؤه بهذه الطريقة (MIele et al., 2022, p20):

$$RaROSI\alpha = \frac{\Delta U[L] - I_0}{I_0} \qquad (3)$$

حيث:

$$\Delta U[L] = E[L] - mCyVaR(\alpha)$$

حيث أن: $E[L]$ هي الخسارة المتوقعة في حين أن $mCyVaR$ هي القيمة السيبرانية المعرضة للخطر، وهي تمثل أسوأ خسارة ممكنة، يخففها الاستثمار في أمن تكنولوجيا المعلومات، وبالتالي فإن $\Delta U[L]$ تمثل تقليل الخسارة المتوقعة بسبب الاستثمار الآمني؛ وتمثل I_0 تكلفة الاستثمار في الأمن السيبراني.

ويلاحظ أن المعايير والتوصيات الصادرة عن الهيئات التنظيمية ذات الصلة، تركز بشكل كبير على الامتثال بدلاً من القياس الكمي للمخاطر السيبرانية(Pollmeier et al., 2023, p1).

ثالثاً: دراسة تحليلية لمتطلبات الإفصاح الالكتروني عن المخاطر السيبرانية وإدارتها في ضوء الأطر والإرشادات التنظيمية.

١/٣- طبيعة وأهمية الافصاح الالكتروني والتقرير عن المخاطر السيبرانية.

يرى (الصاوي، ٢٠٢٢) أن الإفصاح عبر الإنترنت ووسائل التواصل الاجتماعي قد أدى إلى تحسين في بيئة المعلومات من خلال عدة أبعاد، لعل أهمها؛ تحسين الوصول إلى المعلومات، وتخفيض عدم تماثل المعلومات، وتحسين سيولة السوق، وتخفيض مخاطر المعلومات، وزيادة جودة ومستوى الإفصاح والشفافية، وتخفيف رد فعل السوق السلبي. ويعد الإفصاح المحاسبي الالكتروني عن المخاطر السيبرانية من المجالات البحثية التي نالت حيزاً واسعاً في المجال المحاسبي. حيث يضع المحاسبون حوادث الأمن السيبراني ويأخذون في الاعتبار المخاطر السيبرانية أثناء تقييم المخاطر(Hamm, 2019). والإفصاح الالكتروني عن المخاطر السيبرانية هو الإفصاح العام عن المعلومات المتعلقة بحادث أمن البيانات، ويسمح للشركات بإيصال المعلومات البارزة إلى الأطراف المعنية وأصحاب المصلحة فيما يتعلق بطبيعة وتأثير الخرق(Kelton and Pennington, 2020, p139). **والإفصاح الالكتروني عن المخاطر السيبرانية**؛ هو عملية من الإجراءات والضوابط المنطقية التي تمارسها المنظمات للإفصاح عن المعلومات المحيطة بالخرق الأمني، من خلال التأثيرات المختلفة لأصحاب المصلحة، والعوامل الداخلية والخارجية، وغالباً ما تؤدي العملية إلى درجات متفاوتة من الاكتمال والدقة وحسن التوقيت والشفافية ومشاركة الإدارة في المعلومات التي يتم إرسالها إلى أصحاب المصلحة المعنيين لاتخاذ القرارات، واعطاء الفرصة لاستكشاف وفهم الظاهرة والتحقيق في القضايا ذات الصلة (Lee, 2018, p12).

وتكمن **أهمية الإفصاح الالكتروني عن المخاطر السيبرانية** في إظهار جميع المعلومات الضرورية وتلبية احتياجات مستخدمي القوائم المالية عبر موقع الشركة أو إفصاحتها في البورصة وغيرها من التقارير، لمساعدتهم في اتخاذ القرارات، وتخفيض حالة عدم التأكد(يوسف، ٢٠٢٢، ص٤٨-٤٩). ويخصص السوق قيماً سوقية أعلى للشركات ذات الجودة العالية والإفصاحات ذات الصلة بالأمن السيبراني (Berkman et al., 2018). وأن الارتباط الإيجابي بين الإفصاح الالكتروني عن الأمن السيبراني وجاذبية الاستثمار يعتمد على الإفصاح عن مسؤولية الإدارة العليا(Tan and Yu, 2018). وأن المنشآت بحاجة إلى الافصاح عن المخاطر السيبرانية التي واجهتها والمحتملة، لتعزيز الافصاح والشفافية في تقاريرها السنوية(يعقوب وآخرون, ٢٠٢٢، ص ١٤٠٩).

وقد استطاع **الباحث** الوصول الى جميع نماذج الإفصاح التي تلزم بها البورصة المصرية المنشآت المقيدة بها، وقد لوحظ، عدم وجود نماذج للإفصاح عن تقرير المخاطر السيبرانية وإدارتها، وليس هناك نص قانوني يلزمها بذلك، وبالتالي فالمنشآت المقيدة غير ملزمة بالإفصاح عن تقرير المخاطر السيبرانية وحوكمة إدارتها، ويرى **الباحث** أن الإفصاح الالكتروني عن المخاطر السيبرانية هو القدرة على توفير المعلومات لوصف المخاطر السيبرانية، وحوكمة إداراتها والإستجابة لها وتخفيفها في التقرير السنوي، وبيان أثارها الاقتصادية المتوقعة على الأداء الحالي والمستقبلي، لتقليل درجة عدم التأكد الذي يحيط بالخدمات الرقمية في الفضاء السيبراني.

٢/٣- الجوانب الأساسية لمتطلبات الإفصاح الالكتروني عن المخاطر السيبرانية والتقرير عنها

ينبغي أن يشارك المحاسبون في تحديد وقياس تكاليف أحداث الأمن السيبراني؛ وتتبع أثر هذه الأحداث؛ وضمان قيام المنظمات بالإفصاح عن تهديدات وأحداث الأمن السيبراني بشكل مناسب للمستثمرين، وتحسين عملية إدارة المخاطر السيبرانية لزيادة الثقة والشفافية في التقارير المالية، ولذلك أصبحت حماية أصول المعلومات من أهم بنود جدول أعمال المحاسبين (Serag and Daoud, 2022, p21-22).

١/٢/٣- عناصر الإفصاح الالكتروني عن المخاطر السيبرانية: وفقاً لنظرية الإشارة، التي تركز على تقليل عدم تناسق المعلومات بين المديرين وأصحاب المصلحة، يجب على المنشآت تزويد مستثمريها والسوق بمعلومات فورية بشأن أي مخاطر حقيقية تؤثر على أعمالهم، من أجل الحفاظ على برنامج فعال لإدارة المخاطر، وينبغي اعتماد **خمس مراحل**، وهي كالتالي:(١) تحديد مخاطر التعرض للأمن السيبراني وتحديد أولوياتها، (٢) تصميم نظام مراقبة الأمن السيبراني، (٣) اختبار الفعالية التشغيلية لضوابط الأمن السيبراني، (٤)إعداد التقارير الخارجية عن الأمن السيبراني، و(٥) توفير ضمانات بشأن التقارير الخارجية عن الأمن

السيبراني، حيث يمكن لشركات المحاسبة تقديم ضمان رسمي مهني ومستقل بشأن فعالية برنامج إدارة المخاطرالسيبرانية(Newman and Belknap, 2019; Badawy, 2021, p9) . وتتمثل العناصر الأساسية المحيطة بالانتهاكات والمخاطر السيبرانية فيما يلي:-

١/١/٢/٣- الإفصاح الالكتروني عن عامل التهديد وطبيعة التهديد ومواطن الضعف: يستخدم مصطلح عامل التهديد أو ممثل التهديد للإشارة إلى فرد أو مجموعة يمكن أن تظهر تهديداً لسرية موارد النظام وسلامتها وتوافرها، ويمكن لعامل التهديد اتخاذ واحد أو أكثر من الإجراءات التالية ضد أحد الأصول:(الوصول غير المصرح به، والاستخدام غير المصرح به للأصول، والإفصاح عن عامل التهديد بشكل غير قانوني عن معلومات حساسة، والتعديلات أو التغييرات غير مصرح بها على أحد الأصول، ورفض الوصول بما في ذلك التدمير، ومنع الوصول المصرح به)(NIST 800-53, 2019). ومن المهم إدراك أن كل إجراء من هذه الإجراءات يؤثر على الأصول، وتؤثر الإجراءات على الأصول إلى اختلاف طبيعة التهديد، على سبيل المثال، تعتمد احتمالية خسارة الإنتاجية الناتجة عن الأصول المدمرة أو المسروقة على مدى أهمية هذا الأصل في إنتاجية المنشأة وطبيعة الأصل(Lee, 2018, p81). ويمكن للأصول المتعلقة بالمخاطر السيبرانية أن تمثل نقاط ضعف، وتتجسد المخاطر السيبرانية في استغلال نقاط الضعف هذه(Luque et al., 2021, p187). وربطت الأبحاث المحاسبية السابقة بين حوادث الأمن السيبراني ونقاط الضعف المحتملة في الرقابة الداخلية وأوجه القصور في التقارير المالية، وعلى سبيل المثال (Amir et al., 2018; Lawrence et al., 2018; Eaton et al., 2019; Swift et al., 2020; Gao et al., 2020; Nie and Xu, 2021; Rosati et al., 2022; Sebastian, 2022). وهذا الربط يستلزم تضمين إجراءات مراجعة موضوعية لضوابط الأمن السيبراني في SOX ، لضمان مراجعة اختبارات تصميم وفعالية التحكم السيبراني بدقة لتوفير ضمان الأداء السليم لنظام الرقابة الداخلية داخل المنشأة (Sebastian, 2022, p6).

ويري **الباحث** أن نقاط الضعف والثغرات الأمنية التي لم يتم إصلاحها يمكن أن تتسب في مشكلات خطيرة، حيث يهيمن عدد قليل من المنشآت التكنولوجية العالمية الكبري مثل Microsoft و Apple و CISCO و Oracle على صناعة برامج الكمبيوتر والأجهزة؛ وعلى سبيل المثال قد يكون للثغرة الأمنية غير المعالجة في نظام تشغيل واسع الاستخدام مثل Windows XP أو تطبيقات الموبايل عواقب سلبية وخيمة، حيث يمكن أن تؤثر على ملايين المستخدمين والمنشآت أيضاً.

٢/١/٢/٣- الإفصاح الالكتروني عن عمليات الاكتشاف والتحقيق: الاكتشاف هو عملية رصد ومراقبة الأحداث التي تحدث في نظام كمبيوتر أو شبكة وتحليلها بحثاً عن علامات على حوادث محتملة، والتي تمثل انتهاكات أو تهديدات وشيكة بانتهاك سياسات أمان الكمبيوتر أو سياسات الاستخدام المقبولة، ويجب أن تتكون ضوابط الإفصاح في بيئة رقابة سليمة وكافية، والغرض من الإفصاح عند الاكتشاف هو أن يتم إبلاغ توقيت الاقتحام وتوقيت الاكتشاف إلى الأطراف المعنية ذات الصلة Navarro and Sutton, (2021, p281). ويمكن أن يكون الفاصل الزمني بين وقت الحادث ووقت الاكتشاف مؤشراً مهماً لمدى جودة عمل ضوابط الاكتشاف، وبدون هذا الإفصاح لن يتمكن الإفصاح عن الانتهاكات من إبلاغ أصحاب المصلحة المعنيين بالمحتوى التالي من المعلومات:(توقيت ووسيلة وطريقة الاقتحام، وما هو الوقت الذي تستغرقه المنظمة للرد؟، ما هي الإجراءات التي يتم اتخاذها فور اكتشاف الاقتحام؟، وما هي الأطراف المشاركة في عملية الاكتشاف والتحقيق؟)(Lee, 2018, p82).

٣/١/٢/٣- الإفصاح الالكتروني عن تقييم المخاطر وتحليل الأثر: يتيح الإفصاح عن تقييم المخاطر وتحليل الأثر لأصحاب المصلحة المعنيين بالتعرف على الآثار المحتملة للخسارة، وتتيح المعلومات الواردة في تقييم المخاطر وتحليل الأثر لصانعي القرار بتقييم مدى أهمية الحدث وتحديد أولويات التعامل مع الحادث، ويقترح دليل NIST للتعامل مع الحوادث الأمنية الحاسوبية أنه يجب تقييم تأثير الخرق الأمني وفقاً لما يلي:(**الأثر الوظيفي للحادث، وتأثير الحادث على المعلومات، والقدرة على التعافي من الحادث)** (Lee, 2018, p83-84). وأوصى المعهد الأمريكي للمحاسبين القانونيين(AICPA, 2017) لمراقبة الأمن السيبراني بما يلي(Grove and Schaffner, 2019, p93):

١- لتحقيق أهدافه، يستخدم الكيان إجراءات الإفصاح والمراقبة لتحديد(١)التغييرات على التكوينات التي تؤدي إلى إدخال ثغرات أمنية جديدة، و(٢) قابلية التأثر بالثغرات المكتشفة حديثاً.
٢- يقوم الكيان بمراقبة مكونات النظام، وتشغيل تلك المكونات للكشف عن الحالات الشاذة التي تدل على الأفعال الكيدية والكوارث الطبيعية والأخطاء، والتي تؤثر على قدرة الكيان على تحقيق أهدافه، ويتم تحليل الحالات الشاذة لتحديد ما إذا كانت تمثل أحداثاً أمنية.
٣- يقوم الكيان بتقييم الأحداث الأمنية لتحديد ما إذا كان من الممكن أو أدى إلى فشل الكيان في تحقيق أهدافه (الحوادث الأمنية)، وإذا كان الأمر كذلك، يتخذ إجراءات لمنع أو معالجة مثل هذه الإخفاقات.
٤- يستجيب الكيان للحوادث الأمنية التي تم تحديدها، من خلال تنفيذ برنامج استجابة محدد للحوادث، لفهم الحوادث الأمنية واحتوائها ومعالجتها والإبلاغ عنها، حسب الاقتضاء، ويقوم الكيان بتحديد وتطوير وتنفيذ أنشطة التعافي من الحوادث الأمنية التي تم تحديدها.

ووفقاً لإرشادات لجنة الأوراق المالية والبورصات الأمريكية(SEC, 2018)أنه عند مراجعة قواعد الإفصاح الالكتروني عن قضايا الأمن السيبراني يجب مراعاة ما يلي:

١- **الأهمية النسبية:** ينبغي التركيز على توجيه الإهتمام نحو المخاطر السيبرانية عند إعداد تقارير الإدارة السنوية، وخاصة الحوادث الهامة من وجهة نظر المستثمرين والأضرار الناتجة عنها. وتعتمد الأهمية النسبية للمخاطر السيبرانية على مدى الضرر الذي يمكن أن تسببه مثل هذه الحوادث، وهذا يشمل الضرر الذي يلحق بسمعة المنشأة ، والأداء المالي، والعلاقات مع العملاء، وإمكانية التقاضي أو الإجراءات التنظيمية(Zukis, 2022).
٢- **وصف عوامل الخطر السيبراني وطبيعة الأنشطة:** يجب الإفصاح عن الحوادث السيبرانية الفعلية والمتوقعة والتي تمثل مخاطر خاصة على المنشأة في سياق الإفصاح عن إدارة المخاطر السيبرانية، ويجب الإفصاح عن أي حوادث سيبرانية يكون لها تأثير جوهري على طبيعة نشاط المنشأة والعلاقات مع الموردين أو العملاء، ويجب الإفصاح عن أي قضايا متعلقة بإدارتها. وأورد مجلس معايير المحاسبة الدولية (IASB) في "بيان الممارسة العملية المنقح" أنه يمكن أن يوضح تقارير لإدارة المعلومات المتعلقة بوصف ومراقبة المخاطر في مناقشتها، والعوامل التي تؤثر على المخاطر، بما في ذلك احتمال حدوث نتيجة سلبية وتوقيت الاضطراب المحتمل، ويراعي وصف جوانب العمليات الداخلية لمراقبة إدارة المخاطر(IASB, 2020, paragraphs 58(a), p23).
٣- **سياسات الإفصاح في القوائم المالية ونتائج الأعمال:** يجب الإفصاح عن المخاطر السيبرانية التي لها تأثير جوهري على المركز المالي ونتائج الأعمال، وقد تؤثر المخاطر السيبرانية على عناصر القوائم المالية من إيرادات أو مصروفات أو تدفقات نقدية، وبالتالي لابد من الإفصاح عن هذه الأثار ضمن الإيضاحات المتممة للقوائم المالية. وأوضحت دراسة (الرشيدي وعباس، ٢٠١٩، ٤٦١) بأن الإفصاح في القوائم المالية يتأثر بالمخاطر السيبرانية على القوائم المالية للمنشأة؛ حيث يمكن أن تؤدي الى:(زيادة المصروفات المتعلقة بالتحقيق والاخطار بالاختراق وكيفية علاجها، وانخفاض الإيرادات حيث يتعين إما تقديم مزيد من الحوافز للعملاء للحفاظ عليهم وإلا يتم خسارتهم، والمطالبات المتعلقة بالضمانات وعدم الوفاء بالعقد واسترجاع المنتج والتعويضات للأطراف، وانخفاض التدفقات النقدية المستقبلية أو اضمحلال الأصول الفكرية أو غير الملموسة، وغيرها من الأصول فضلاً عن الاعتراف بمزيد من الالتزامات وزيادة تكاليف التمويل).
٤- **دور مجلس الإدارة:** يجب الإفصاح عن دور مجلس الإدارة بخصوص برنامج إدارة المخاطر السيبرانية، والذي يؤثر إيجاباً على المستثمرين، وعلى الرغم من عدم وجود تنظيم حصري للإفصاح عن معلومات الأمن السيبراني في التقرير السنوي، إلا أن بعض اللوائح الصادرة عن كيانات الإشراف والرقابة فيما يتعلق بحوكمة المنشآت وإدارة المخاطر وخصوصية البيانات أدت إلى زيادة الإفصاح عن الأمن السيبراني(Ramírez et al., 2022,p7).

ويرغب المستثمرون في الإفصاحات عن الآتي: (ربط حوكمة التحول الرقمي والمخاطر الأمنية بالاستراتيجية والرغبة في المخاطرة؛ وتوضيح كيفية قيام مجلس الإدارة واللجان التابعة له بالإشراف على هذه المخاطر؛ والنظر في الإجراءات والأنشطة المتخذة للتخفيف من المخاطر وكيفية تطور المخاطر؛ وتوفير معلومات عن المخاطر وعمليات التخفيف من حدتها؛ وربط الأمن والاستراتيجية الرقميين

بالإفصاح عن المرونة السيبرانية، وإبراز تأثيرات الأحداث (الداخلية والخارجية)، وعلى وجه التحديد ، في حالة تعرض المنشأة لحادث إلكتروني، تقوم بتوفير معلومات حول(الحادث وآثاره المباشرة، والتخفيف من الإجراءات المتخذة وأهدافها وفعاليتها، وعمل المجلس لتسهيل التعافي من الحادث، والتأثير المالي المحسوب للحادث، وأي تحسينات سيتم إجراؤها استجابة للحادث (FRC, 2022, p4-8).

ولقد حددت هيئات الرقابة الداخلية (SSBs) لمعالجة الإشراف على المخاطر الإلكترونية على أنها أولوية قصوى، ولقد استندت هيئات الرقابة الداخلية بما في ذلك لجنة بازل ، و CPMI-IOSCO ، و IAIS إلى الأطر التنظيمية الحالية لإدارة المخاطر التشغيلية مع التوجيه التكميلي للفضاء السيبراني، وتركز الإرشادات التكميلية على جوانب إدارة المخاطر الخاصة بالفضاء السيبراني، مثل مشاركة المعلومات، والإبلاغ عن الحوادث وما إلى ذلك، وقد وضعت هيئات الرقابة الإدارية متطلبات لإدارة المخاطر التشغيلية عالية المستوى بطبيعتها وتغطي القضايا المتعلقة برقابة مجلس الإدارة والإدارة والأمن، والضوابط، وإدارة المخاطر القانونية والمتعلقة بالسمعة، واستمرارية الأعمال والتخطيط للطوارئ، وإدارة الأنشطة الخارجية بالإضافة إلى التوجيه المستهدف لاستكمال المتطلبات العامة لإدارة المخاطر التشغيلية وموضوعات محددة مثل استمرارية الأعمال والتعافي من الكوارث(Gaidosch et al., 2019, p11).

٤/١/٢/٣- الإفصاح الالكتروني عن العلاج والاحتواء والرقابة التصحيحية والوقائية: إن الاحتواء، والضوابط التصحيحية هي عناصر مهمة في الإفصاح، ويشير إلى أن المنشأة على رأس الانتهاك وقادرة على احتواء ومنع الحوادث المستقبلية، ويمكن أن يشمل الإفصاح عن ضوابط الاحتواء والرقابة التصحيحية والوقائية، ما يلي:(إجراءات لمنع الضرر المحتمل للموارد وسرقتها، وإجراءات للحفاظ على توافر الخدمات (مثل الربط الشبكي والخدمات المقدمة إلى أطراف خارجية)، وفعالية الاستراتيجية (مثل الاحتواء الجزئي والكامل)، ومدة الحل(على سبيل المثال، حل الطوارئ المراد إزالته في غضون أربع ساعات، والحل المؤقت الذي يتعين إزالته في غضون أسبوعين، والحل الدائم) (Lee, 2018, p85).

وأوصى معهد المحاسبين القانونيين(AICPA, 2017) لمراقبة الأمن السيبراني وتخفيف المخاطر بأن يقوم الكيان بتحديد وتطوير أنشطة التخفيف من المخاطر الناشئة عن الاضطرابات التجارية المحتملة، وأن يقوم الكيان بتقييم وإدارة المخاطر السيبرانية(Grove and Schaffner, 2019, p94). ويجب أن تضمن إجراءات الإفصاح أن المعلومات المتعلقة بالمخاطر السيبرانية تتم معالجتها والإفصاح عنها(PwC, 2018). ويجب أن تشكل الموضوعات التالية الأساس للتنظيم الفعال للأمن السيبراني لجميع المنشآت ومنها:(إسناد مسؤوليات إدارة المخاطر السيبرانية إلى مجلس الإدارة؛ برنامج وحوكمة الأمن السيبراني الموثق، وتحديد أصول المعلومات الهامة والتهديدات السيبرانية، ومنع البرمجيات الخبيثة؛ والمراجعات الأمنية (مثل عمليات فحص الثغرات الأمنية، واختبار الاختراق)، واستمرارية الأعمال وتكنولوجيا المعلومات والاتصالات والمرونة التشغيلية، وإدارة مخاطر الاستعانة بمصادر خارجية، والإبلاغ عن الحوادث السيبرانية، وعدد ومعرفة المتخصصين في الأمن السيبراني، الأمن المادي وأمن الشبكة) (Gaidosch et al., 2019, p10).

ويرى الباحث، أنه من الضروري التحقق من جودة الإفصاح الالكتروني عن المخاطر السيبرانية، وأن يتضمن الإفصاح الالكتروني معلومات ذات قيمة لمتلقيها، لمساعدة أصحاب المصلحة على اتخاذ القرارات بعد حدوث الخرق الأمني، وتتعلق بوصف مصادر التهديد والغرض منه، وطبيعة الأحداث والآثار المحتملة والحل المحتمل، ويجب أن تكون لدى المنشآت سياسات وضوابط أمنية كافية، لتمكين الإفصاح الداخلي عن المشاكل الأمنية بحيث يتم إبلاغ الإدارة العليا ومجلس الإدارة بشفافية، وأن تسعى الإدارة العليا إلى الإشارة لمسؤوليتها تجاه أصحاب المصلحة، وذلك لتحقيق مجالات جودة الإفصاح عن المخاطر السيبرانية الثلاثة، (الاكتمال وحسن التوقيت ومدى مشاركة الإدارة عموماً في عملية الإفصاح عن المخاطر السيبرانية).

٢/٢/٣- الإفصاح الالكتروني الداخلي والخارجي عن المخاطر السيبرانية

١/٢/٢/٣- الإفصاح الالكتروني الداخلي عن المخاطر السيبرانية: يعتبر الإفصاح جزءاً أساسياً من عملية إدارة الاستجابة للحوادث، لذلك عند وقوع حادث أمني، يمكن لأعضاء المنظمة اتباع إجراءات محددة للتحقق والإبلاغ عن الحادث، ويجب أن يدرك مجلس الإدارة أو الأشخاص المسؤولون عن الحوكمة، أن الإدارة قد

تتجنب الإفصاح الداخلي إذا أدركوا عواقب سلبية محتملة على مراجعة أدائهم (Eijkelenboom and Nieuwesteeg, 2021, p8).

- **الإخطار الأولي:** بعد وقوع حادث أمني، يمكن للمنظمة اتخاذ تدابير مختلفة لإخطار الأطراف الخارجية بالحوادث الأمنية، وتتطلب بعض الجهات التنظيمية إخطاراً أولياً "فورياً" للجهة التنظيمية، وتنص لائحة(GDPR)،على أنه يجب تقديم إخطار أولي إلى الجهة المنظمة في غضون ٧٢ ساعة، والفروق بين توقيت الإفصاح وموثوقيته هي مجال يجتذب البحوث في مجال المحاسبة المالية، فيما يتعلق بالإفصاح عن الخرق الأمني، حيث أن تقييم الخرق سوف يتحسن مع مرور الوقت Lee, 2018, p36).
- **إخطار العميل / الفرد:** أصبحت اللوائح الخاصة بمتطلبات إخطار خرق البيانات للعملاء المتضررين أكثر إلزاماً، وعندما ينطوي الخرق الأمني على فقدان البيانات، وعادة ما يطلب المنظمون الإفصاح عن الواجهة الخارجية للطرف المتضرر، ويعد الاتصال الخارجي مع العميل بعد الخرق مكوناً مهماً في الاستجابة للحوادث، وترسل إشارة قوية حول قدرة المنظمة على مواجهة الأحداث السلبية والاحتفاظ بثقة عملائها، والغرض الأساسي من الإفصاح عن الخرق الفردي هو مساعدة الأفراد المتضررين على فهم المشكلة بحيث يمكن اتخاذ الخطوات المناسبة لمنع المزيد من الضرر (Masuch, et al., 2022, p17).

٢/٢/٢/٣- الإفصاح الالكتروني الخارجي عن المخاطر السيبرانية: قد لا يتم الإفصاح عن حادث أمني علنًا، إذا لم يتم استيفاء الشروط التالية(Lee, 2018, p27):

- يجب أن يتم اكتشافه من خلال التحكم في الإفصاح أو المصادر الخارجية؛ ويجب الإبلاغ عنها داخلياً إلى أعلى (الإدارة) ومن أسفل (الموظفين) المسؤولين عن الاستجابة للحوادث؛ ويجب أن تستوفي الشروط التي تستدعي الإفصاح الخارجي؛ وهذا يرجع إلى حقيقة أنه لا تؤدي جميع الحوادث الأمنية إلى خرق البيانات الشخصية أو "ضرر متوقع" للطرف المتضرر؛ ويجب أن تكون خالية من تقدير الإدارة أو التدخل المتعمد في الإفصاح العلني عن معلومات الخرق.

وإذا لم يتم استيفاء أي من الشروط الضرورية **الأربعة** المذكورة أعلاه، أو لم يتم توضيح المسؤوليات، فمن المحتمل أن يقع الحادث الأمني ولا يتم الإفصاح عنه، وفي حالة تدخل الإدارة يمكن أن يأتي في شكل التلاعب في عملية إعداد التقارير الداخلية لتجنب الإفصاح الداخلي، أو التلاعب في تقييم الأثر الذي من شأنه أن يغير التأثير بحيث لا يستوفي شرط الإفصاح الخارجي، أو تجنب الإفصاح. وقد تفكر فرق إعداد تقارير المنشآت التي ترغب في تعزيز عمليات الإفصاح وتلبية احتياجات المستثمرين في الإفصاح عما يلي:(شرح مدى أهمية الأمن الرقمي والاستراتيجية الرقمية لنموذج عمل المنشأة الحالي والمستقبلي، وتفاصيل هياكل الحوكمة والثقافة السيبرانية والعمليات التي تطبقها المنشأة لدعم الأمن الرقمي والاستراتيجية، وتحديد مخاطر الأمن الرقمي والاستراتيجيات والفرص التي تواجهها المنشأة الآن وفي المستقبل(FRC, 2022, p3). وأوصي فريق عمل مجلس معايير المحاسبة الدولية (IASB) في أجندته في مايو ٢٠٢٠في ملخص بيان توصيات المجلس "بيان االممارسة العملية المنقح" بما يلي(IASB, 2020, p2-3**:((أ)**يحدد هدف الإفصاح عن المخاطر على النحو التالي:(يجب أن يوفر تعليق الإدارة معلومات وتحليلات لمساعدة المستثمرين والدائنين على فهم المخاطر، التي يمكن أن تعطل نموذج أعمال الكيان، وتساعد هذه المعلومات والتحليلات المستثمرين والدائنين على تقييم:(١) حجم واحتمال حدوث اضطراب(تعطيل) مستقبلي محتمل في قدرة المنشأة على خلق القيمة، و (٢) مدى فعالية الإدارة في تحديد المخاطر وإدارتها، و يجب أن تركز تلك المعلومات والتحليلات على المخاطر الرئيسية على ما يلي: (١) وصف للمخاطر ومدى تعرض المنشأة لتلك المخاطر؛ و(٢) كيف تقوم الإدارة بمراقبة وإدارة المخاطر، وإمكانية التخفيف من الاضطراب في حالة حدوثه)، **و(ب)** يحدد الكيان أن المخاطر الرئيسية التي يمكن أن تعطل قدرة المنشأة على خلق القيمة وتوليد التدفقات النقدية).

ويترتب على الرقمنة عدة أنواع من المخاطر من أهمها مخاطر الاستعانة بالمصادر الخارجية، والمخاطر السيبرانية ومخاطر التشغيل الأخرى، والتي يجب الإفصاح عنها بحد أدنى عن البيانات التالية مع مقارنتها بالفترة المالية السابقة على أن يكون الإفصاح كافياً، وذلك على **النحو التالي**: (استراتيجية

التحول الرقمي وعلاقاتها مع الاستراتيجية العامة للمنشأة ، وخطط وإجراءات تأمين الأنظمة والبيانات الخاصة، وتوعية العملاء بالخدمات الرقمية، والإجراءات التصحيحية التي اتخذتها المنشأة بسبب الاختراقات الأمنية والقراصنة، وعدد حالات الاختراق المرتبطة بأمن البيانات، وعدد حالات الدخول غير المصرح بها والناتجة عن إخفاقات الموظفين أو العمليات أو أوجه القصور في الأنظمة و التكنولوجيا، والنسبة المئوية لانتهاكات أمن البيانات التي تتضمن المعلومات الشخصية غير المشفرة للعملاء، وخطط تدريب الكوادر البشرية) (عقل، زهري،٢٠٢٠، ص٢٢٧-٢٢٨؛ على، ٢٠٢٢، ص٤٤١-٤٤٣).

ويجب على **فرق الإبلاغ و الإفصاح عن المخاطر السيبرانية** مراعاة ما يلي (FRC, 2022, p4-8):

- **عمليات الإفصاح الأساسية**، وتشمل: (الرجوع إلى الأهداف الاستراتيجية والرغبة في المخاطرة وبيان الجهة المالكة لكل خطر؛ وتقديم تفاصيل عن الأطر وعمليات التخفيف والإجراءات، وتحديد العناصر التي تنعكس على نطاق المجموعة أو تسلط الضوء على مجالات محددة من الأعمال التجارية التي تتأثر، وتوفير معلومات حول طبيعة الحادث وتأثيراته المباشرة.
- **عمليات الإفصاحات المحسنة(المعززة)**، وتشمل:(تقديم تقارير عن الفرص والتهديدات، وتحديد الفرص وتوفير روابط واضحة ومحددة لسيناريوهات القدرة على الاستمرارية والمرونة، وتقديم تفاصيل عن السيناريوهات السيبرانية،(مثل طول فترة الاضطراب، والتكلفة، والاستجابة التنظيمية).

ومن بين **اعتبارات أخرى**، يتطلب من المنشآت عند الإفصاح عن المخاطر السيبرانية مراعاة ما يلي:(استعداد المنشأة التشغيلي والمالي لحدوث اضطراب في أعمالها؛ وقدرة المنشأة على إدارة المخاطر السيبرانية؛ واحتمالية المخاطر وتأثيرها على عمليات المنشأة وصحتها المالية؛ والإجراءات المخففة التي وضعتها المنشأة لإدارة المخاطر السيبرانية) (FRC, 2022, p9). **ويجب** عدم الإفصاح عن المعلومات المتعلقة بالمخاطر السيبرانية بشكل إنتقائي**(الإفصاح الإنتقائي)**(SEC, 2018). ووفقا للنسخة الصادرة عن(SEC)في مارس ٢٠٢٢، يجب على المنشآت تقييم الأهمية الجوهرية المحتملة لأي مخاطر محددة وفي حالة الحوادث السيبرانية، وأي معلومات تم اختراقها وتأثير الحادث على عمليات المنشأة (SEC, 2022).

وفي ضوء **تعليمات البنك المركزي المصري** يجب على البنك الإفصاح عن الإطار العام لإدارة مخاطر التشغيل لديه بالشكل الذي يسمح بالمتعاملين معه في تحديد مدى قدرة البنك على تحديد وتقييم ومراقبة والتحكم في مخاطر التشغيل لديه، ويجب القيام بالإفصاح بشكل كافي عن حجم الخسائر الناجمة عن مخاطر التشغيل لديه بما يسمح لكافة الأطراف بالسوق بتقييم الأسلوب المتبع من قبل البنك لإدارة مخاطر التشغيل، ويجب أن يكون حجم البيانات والمعلومات المفصح عنها المتعلقة بمخاطر التشغيل تتناسب مع حجم البنك وتعقد عملياته وأنشطته والإطار العام للمخاطر لديه(البنك المركزي المصري، ٢٠٢١، ص٥). وينعكس ذلك على تصميم نظم التقرير المالي، لتوفير تأكيد معقول بأن المعلومات الخاصة بنطاق وحجم التأثيرات المالية لحوادث الأمن السيبراني تم أخذها بعين الاعتبار عند اعداد القوائم المالية، وتأسيساً لما تقدم فإن استجابة الوحدات الاقتصادية للإفصاح عن المخاطر السيبرانية يعد الركيزة الأساسية، للمحافظة على الثقة ومصداقية التقارير المرفقة للتقارير المالية، والمتعلقة بالإفصاح عن المخاطر السيبرانية التي توليها الجهات المحاسبية والرقابية الاهتمام المتزايد، دورياً(سنوياً) (يعقوب وآخرون, ٢٠٢٢، ص ١٤١٤).

رابعاً: جهود المؤسسات التنظيمية والرقابية للفكر المحاسبي في الإفصاح الالكتروني عن المخاطر السيبرانية

زادت الاهتمام من قبل الهيئات المهنية المحاسبية والمنظمة للإفصاح في الأسواق المالية حول المخاطر السيبرانية، خاصةً بعد التهديدات والخروقات الكبيرة التي تعرض لها المنشآت بكافة القطاعات(يعقوب وآخرون, ٢٠٢٢، ص ١٤٠٩). وعلى ذلك أصدرت العديد من الهيئات إصدارتها بهذا الشأن، كالتالي:

١/٤- تحليل جهود الهيئات والاصدارات المهنية في الإفصاح عن المخاطر السيبرانية.

١/١/٤- المعهد الأمريكي للمحاسبين القانونيين(AICPA): قدم دليلا للإفصاح الاختياري عن المخاطر السيبرانية في ٢٩ أبريل ٢٠١٧ من خلال اصدار معايير لوصف الأسلوب، والذي يتم من خلاله تبني سياسات وإجراءات احترازية للوصول الى إدارة مخاطر أمن سيبرانية فاعلة، والافصاح عن المؤشرات التي تمكن مستخدمي معلومات تقرير المخاطر السيبرانية من فهم المخاطر والأسلوب التي يتم ادارته بها، ويساعد الاطار المقدم من قبل(AICPA)في تحديد خطوات اعداد تقارير إدارة المخاطر السيبرانية، فضلاً عن خدمات المراجعة المرافقة له، وحدد(AICPA) التقرير الذي تلتزم به المنشآت (طوعياً للإفصاح عن المخاطر السيبرانية) (يعقوب وآخرون, ٢٠٢٢، ص١٤٠٩ Haapamäki and Sihvonen, 2019, p810;).

ويتكون التقرير المتعلق بالإفصاح الاختياري للشركات عن المخاطر السيبرانية من ثلاثة أقسام(عثمان، ٢٠٢٢، ص٨-٩؛ يعقوب وآخرون, ٢٠٢٢، ص ١٤١١؛ على، على، ٢٠٢٢، ص٩-١١ (AICPA, 2017 a, 2017 b, 2018 ; Eaton et al., 2019, c3; AKÇAKANAT et al., 2021, p255-256; Grove and Schaffner, 2019, p89-91; Peng and Li, 2022, p458-459; Elsherif, 2022, p3;). يتكون **القسم الأول: معايير الوصف**(Management's description)، لكي يستخدمها مجلس الإدارة عند تنفيذ برامج إدارة مخاطر الأمن الإلكتروني، وهي عبارة عن وصف سردي تعده إدارة المنشأة ، لوصف برنامج إدارة المخاطر السيبرانية. ويتكون **القسم الثاني** تأكيد إدارة(Manageinent's assertion)الوحدة الاقتصادية بأن تقرير الإفصاح عن المخاطر السيبرانية قد تم إعداده وفقاً لـ(AICPA)، وأن الضوابط الرقابية كانت وفق برنامج إدارة المخاطر السيبرانية، ويتكون **القسم الثالث** من رأي الممارسين(The practitioner's opinion)، ويتضمن مراجعة تقرير إدارة المخاطر السيبرانية الذي تم إعداده من قبل إدارة المنشأة ، وتقييم ما إذا كانت الضوابط الرقابية داخل برنامج إدارة المخاطر السيبرانية للمنشأة فعالة، والتحقق من تحقيق أهداف الأمن السيبراني المتمثلة في الحفاظ على سلامة وسرية وتوافر المعلومات، ومن ثم الحصول على أدلة إثبات كافية ومناسبة لتوفير أساس معقول لرأيه بشأن تقرير إدارة المخاطر السيبرانية للمنشأة.

٢/١/٤- معهدي سنغافورة للمحاسبين القانونيين المعتمدين: يصف معهد سنغافورة للمحاسبين القانونيين(ISCA, 2018)بأن المخاطر السيبرانية ذات صلة بكل كيان تقريباً، سواء كان كبيراً أو صغيراً، مع أو بدون منصة عبر الإنترنت، والمخاطر السيبرانية هي منطقة مخاطر لا تقل أهمية ولا يمكن تجاهلها، ويمكن أن تؤدي الحوادث السيبرانية إلى عواقب مالية، وبالتالي يكون لها تأثير على البيانات المالية، ويمكن أن تمر الهجمات الإلكترونية دون اكتشاف، مما يؤدي إلى آثار مالية على الكيان ربما لم يتم عكسها في البيانات المالية(ISCA, 2018, p5). وينبغي تشخيص الاستعداد للأمن السيبراني والذي يهدف إلى تقييم فعالية تدابير الأمن السيبراني الحالية وتقييم مدى استعداد الكيان في إدارة المخاطر السيبرانية، ويعد تشخيص الاستعداد للأمن السيبراني اختباراً أكثر شمولاً، وغالباً ما يشتمل على متخصصين ذوي خبرة عميقة ويركز على المخاطر السيبرانية وعمليات وضوابط الكيان ككل، ويشمل اختبار الفعالية التشغيلية للضوابط التي تخفف من المخاطر السيبرانية بما في ذلك الأمور التشغيلية وغيرها من الأمور غير ذات الصلة بالتقارير المالية(ISCA, 2018, p7).

٢/٤- تحليل القواعد التنفيذية للمرونة السيبرانية لمعالجة في ضوء مقررات لجنة بازل

أصدر مكتب الإشراف على المؤسسات المالية(OSFI)التقرير الاستشاري للإبلاغ عن حوادث الأمن السيبراني والتكنولوجي ومتطلبات الإخطار الأولية والتقارير اللاحقة في ١٦ أغسطس ٢٠٢١ للمؤسسات المالية ، وإن الحادث المطلوب الإفصاح عنه له **خصائص** منها:(التأثير على عمليات البنك والبنية التحتية

وعلى سرية وسلامة ونزاهة البيانات، التأثير التشغيلي على المستخدمين الداخليين أو العملاء الخارجيين أو السمعة، التأثير الذي يلحق بطرف ثالث)، ويجب الإبلاغ عن الحادث خلال ٢٤ ساعة، وتقديم تحديثات لتوفير جميع التفاصيل حول الحادث، اعتماداً على شدة الحادث وتأثيره وسرعته(OSFI, 2021, p1, 3).

وأصدرت لجنة بازل للرقابة المصرفيةBCBS عام ٢٠١٨ تحت إشراف بنك التسويات الدولية(BIS)ملخص تنفيذي لممارسات المرونة السيبرانية، ويتضمن ما يلي:-

١/٢/٤- التنظيم والإشراف: يتوقع المنظمون من البنوك معالجة المخاطر السيبرانية إما في أطر إدارة المخاطر و/أو أمن المعلومات أو في استراتيجياتها المحددة للأمن السيبراني، ويشمل هذا **الأخير** ما يلي:(المتطلبات المتصلة بالإدارة والرقابة؛ وملكية المخاطر والمساءلة؛ وأمن المعلومات؛ والتقييم والمراقبة الدوريان لضوابط الأمن السيبراني؛ والتصدي للحوادث؛ واستمرارية الأعمال؛ وخطط الانتعاش والتعافي)، ويقوم المشرفون بتقييم ضوابط الأمن السيبراني للبنوك ورصد ومراقبة التهديدات، ومراجعة تقارير اختبار التحكم واختبار الاختراق(BIS, 2021, p1).

٢/٢/٤- معايير المرونة السيبرانية وإرشاداتها: تستخدم(BCBS)تعريف المرونة السيبرانية لمجلس الاستقرار المالي(FSB)على أنها "قدرة المنظمة على الاستمرار في تنفيذ مهمتها من خلال توقع التهديدات السيبرانية والتكيف معها والتغييرات الأخرى ذات الصلة في البيئة ومن خلال تحمل الحوادث السيبرانية واحتوائها والتعافي منها بسرعة "(BIS, 2021, p1).

وتغطي توقعات المرونة السيبرانية، التي يتم تضمينها أحياناً في إرشادات مخاطر تكنولوجيا المعلومات، مجموعة واسعة من المعايير التنظيمية، وتتناول **الإرشادات** عادةً الحوكمة وإدارة المخاطر وأمن المعلومات واستعادة تكنولوجيا المعلومات وإدارة ترتيبات الاستعانة بمصادر خارجية لتكنولوجيا المعلومات، وتساهم **المعايير** المتعلقة بمواضيع المخاطر العامة مثل تخطيط استمرارية الأعمال والاستعانة بمصادر خارجية في إدارة مجموعة واسعة من المخاطر ولها صلة أيضاً بالمخاطر السيبرانية ويشجع المشرفون الكيانات الخاضعة للتنظيم على تنفيذ المعايير الدولية وتطبيق التوجيهات والممارسات الاشرافية المتوافقة مع المبادرات الوطنية، ومن المعايير الدولية والصناعية مثل NIST و ISO / IEC و COBIT .(BCBS, 2018, P9)

٣/٢/٤- مناهج إدارة المخاطر والاختبار والاستجابة للحوادث السيبرانية والتعافي منها: يتوقع المنظمون أن تضع البنوك إطاراً للاستجابة للحوادث والتعافي منها، وقد يشمل متطلبات استمرارية الأعمال الإلكترونية ومتطلبات التعافي من الكوارث، لمساعدة المؤسسات المالية على تعزيز ممارساتها في هذا المجال، أصدر FSB في عام ٢٠٢٠ تقريراً بعنوان الممارسات الفعالة للاستجابة لحوادث الإنترنت والتعافي منها والذي يوفر مجموعة أدوات تضم ٤٩ ممارسة عبر المكونات السبعة التالية:(الحوكمة، والتخطيط والإعداد، والتحليل، والتخفيف، والاستعادة والإنتعاش، والتنسيق والاتصال، والتحسين)(BIS, 2021, p2). ويصنف هذا القسم إلى **أربعة أقسام** فرعية: (طرق الإشراف على المرونة السيبرانية، واختبار ضوابط أمن المعلومات والضمان المستقل(مثل اختبار الاختراق، وتصنيف ضوابط المخاطر السيبرانية)، واختبار وممارسة الاستجابة والاسترداد(مثل تقييم استمرارية الخدمة والاستجابة وخطط التعافي والتعليم المستمر)، ومقاييس الأمن السيبراني والمرونة(مثل أولويات تكنولوجيا المعلومات، والأدوار والمسؤوليات، وأصول تكنولوجيا المعلومات، والإرتباط مع أطراف ثالثة))(BCBS, 2018, p16).

٤/٢/٤- الحوكمة السيبرانية في ضوء مقررات لجنة بازل: أصدرت غالبية الجهات التنظيمية إما إرشادات قائمة على المبادئ أو لوائح توجيهية، بمستويات متفاوتة من النضج، وبشكل عام، تتناول المعايير التنظيمية والممارسات الإشرافية إدارة مخاطر تكنولوجيا المعلومات في المؤسسة ولكنها لا تشمل لوائح أو ممارسات إشرافية محددة تغطي إدارة المخاطر السيبرانية للوظائف التجارية الحيوية أو الترابط أو إدارة المخاطر من قبل طرف ثالث، وفي ظل هذه الخلفية، تم تحديد وتحليل التوقعات والممارسات الإشرافية في المجالات التالية ذات الصلة **بالحوكمة**:(استراتيجية الأمن السيبراني، وأدوار ومسؤوليات الإدارة، وثقافة التوعية

بالمخاطر السيبرانية، والهندسة المعمارية والمعايير، والقوى العاملة في مجال الأمن السيبراني) BCBS, (2018, p11).

٥/٢/٤- الترابط مع الأطراف الثالثة: يتم تحليل ممارسات المرونة السيبرانية فيما يتعلق بالأطراف الثالثة عبر المجالات التالية: (حوكمة الروابط المتبادلة بين أطراف ثالثة، واستمرارية الأعمال وتوافرها، وسرية المعلومات ونزاهتها عند التعامل مع أطراف ثالثة، والتوقعات والممارسات المحددة فيما يتعلق برؤية علاقات الترابط مع الأطراف الثالثة، والمراجعة والاختبار، والموارد والمهارات)(BCBS, 2018, p30).

٦/٢/٤- مقاييس المرونة السيبرانية: ركزت المقاييس على استخدام المعلومات المستمدة من الحوادث المبلغ عنها، وأنشطة الاختبار، وهناك اعتراف بالحاجة لتطوير المزيد من مقاييس المرونة السيبرانية BIS, (2021, p3). ويوضح الجدول رقم(١) مقاييس المرونة السيبرانية كالتالي:

جدول رقم(١)

مقاييس المرونة السيبرانية في ضوء مقررات لجنة بازل

	الحدث	الممارسات
قبل التسوية	• مسح خارجي للاتصالات المحظورة (العدد) • ثغرات أمنية جديدة (حسب نوع OWASP: العدد) • توقفت البرامج الضارة (العدد) • مواقع التصيد المعروفة (العدد) • إزالة موقع التصيد الاحتيالي (العد، ساعات فتح الموقع) • بنك فريد من نوعه يستهدف البرامج الضارة (العدد) • نقاط الضعف لكل كود من التعليمات البرمجية (العدد) • التطبيقات قيد الإنتاج مع وجود ثغرات في التعليمات البرمجية (العدد) • الكشف عن الأحداث الأمنية (العدد)	• اختبار الاختراق (حسب النوع: العد وإيجاد التصنيف) • الأنظمة المحمية بواسطة IAM (عدد) • الأنظمة المطورة داخلياً والتي لا يمكن تحديثها (حسب النوع: العدد) • أنظمة مزودة بعناصر دعم من خارج البائعين(حسب النوع: العدد) • أنظمة بدون حلول لمكافحة البرامج الضارة (العدد) • الأجهزة غير المصرح بها (المتوافقة) (العدد) • تمارين التوعية (نسبة التغطية، العدد) • استجابة الموظفين لاختبارات التصيد(النسبة المئوية من مجموع الموظفين) • مراجعة وصول المستخدم (نسبة التغطية ٪) • التقييمات الأمنية لمقدمي الخدمات على مدار ١٢ شهراً(النسبة المئوية لتغطية الأطراف الثالثة ذات الصلة) • تقرير تأكيد بشأن أمن المعلومات (النتائج حسب التصنيف، والتقادم حتى الإصلاح)
التسوية	• نقاط نهاية البرامج الضارة المكتشفة(العدد) • البرمجيات الضارة المكتشفة على الخوادم(العدد) • أدلة على الإنترنت تحتوي على معلومات عن الموظفين/العملاء(العدد) • نوع الحادث على مدار الفترة(العدد حسب: رفض الخدمة، تعليمات برمجية ضارة(رمز خبيث)، إساءة استخدام، استطلاع، هندسة اجتماعية، وصول غير مصرح به، أخرى)	• وضع خطط القرار والاسترداد(حسب النوع: العدد) • التدريبات على الحوادث (حسب النوع: العدد)
بعد التسوية	• تم اكتشاف أداة الحزم المتقدمة APT لتثبيت برامج أو ملفات ضارة (عدد) • الاتصالات المحظورة إلى مواقع الويب الضارة (العدد) • الكشف عن انتهاكات البيانات (العدد) • الخسائر المصرفية (القيمة) • خسارة العملاء (القيمة)	• التقارير اللاحقة(ما بعد الحوادث) (العدد)

Resource :BCBS, 2018, p45.

٣/٤- تحليل جهود منظمي الأسواق المالية والمنشآت في الإفصاح عن المخاطر السيبرانية.

أصدر مجلس إدارة المنظمة الدولية لهيئات الأوراق المالية(IOSCO)[١] في ١٨ يونيو ٢٠١٩تقريراً نهائياً، يقدم لمحة عامة عن ثلاثة معايير وأطر عمل إلكترونية معترف بها دولياً، ويستخدمها أعضاء المنظمة الدولية لهيئات الأوراق المالية(IOSCO)، كما تحدد الثغرات المحتملة في تطبيق هذه المعايير وتسعى إلى تعزيز الممارسات السيبرانية السليمة عبر أعضاء المنظمة، والغرض منه هو أن يكون بمثابة مصدر لمنظمي الأسواق المالية والمنشآت، وزيادة الوعي بالمعايير والأطر الإلكترونية الدولية الحالية، وتشجيع تبني الممارسات الجيدة للحماية من المخاطر الإلكترونية(IOSCO, 2019).

١/٣/٤- إرشادات لجنة الأوراق المالية والبورصات الأمريكية(SEC) : أصدرت دليل استرشادي بمتطلبات الإفصاح عن المخاطر السيبرانية عام ٢٠١٨، وسبقته دليل لعام٢٠١١، وتقترح الـ(SEC) بغرض الإفصاح الالزام في تقرير منفصل أو مدمج مع تقارير المنشأة وتقترح أن تكون مع تقرير تعليقات الإدارة، وترى أن هذا الإفصاح سيعزز في قدرة المستثمرين على تقييم ممارسات الأمن السيبراني للشركات والابلاغ عن الحوادث السيبرانية والاختراقات، بحكم أنها فرصة لجعل المستثمرين يقرروا عن أي مخاطر التي يرغبون بتحملها، واعتبرت المخاطر السيبرانية من المخاطر الناشئة ولها تأثيرات مالية وتشغيلية وقانونية والحاجة الى تقارير عن الاحداث الجوهرية للمخاطر السيبرانية(فرج, ٢٠٢٢، ص ١٤٠- ١٤٢؛ يعقوب وآخرون, ٢٠٢٢، ص ١٤٠٩؛ (SEC, 2011, 2018; Auman, 2018, p957-961; Gao et al., 2020, p2; Héroux and Fortin, 2020, p78; Swift et al., 2020, p197; Jasa, 2020, p9; Chen et al., 2022, p3-4; Sebastian, 2022, p5; Florackis et al., 2023, p361;

وأصدرت لجنة الأوراق المالية والبورصات الأمريكية(SEC)مجموعتين من الإرشادات التفسيرية بشأن الإفصاح عن المخاطر السيبرانية، ودعا **التوجيه الأول**، بعنوان إرشادات الإفصاح عن الأمن السيبراني **(Topic No. 2: Cybersecurity)** المنشآت للإفصاح عن:((١)جوانب الأعمال أو العمليات التي تؤدي إلى مخاطر جوهرية على الأمن السيبراني والتكاليف والعواقب المحتملة؛ (٢) وظائف الاستعانة بمصادر خارجية التي تنطوي على مخاطر جوهرية للأمن السيبراني ومعلومات عن كيفية معالجة المنشأة لتلك المخاطر؛ (٣) وقوع الحوادث السيبرانية التي تكون جوهرية فردية أو إجمالية، بما في ذلك معلومات عن التكاليف والعواقب؛ (٤) المخاطر المتعلقة بالحوادث السيبرانية التي قد تظل غير مكتشفة لفترة طويلة؛ و(٥) المعلومات المتعلقة بالتغطية التأمينية للأمن السيبراني)(SEC, 2011). ودعا **التوجيه الثاني**، في عام ٢٠١٨ المنشآت لإتخاذ جميع الإجراءات المطلوبة لإبلاغ المستثمرين بمخاطر وحوادث الأمن السيبراني الجوهرية في الوقت المناسب، ويُنصح المنشآت بمراجعة المجالات التالية عند تقييم المخاطر السيبرانية وحوادث الأمن السيبراني لعمليات الإفصاح: ((١) وقوع الحوادث الإلكترونية؛ ٢) احتمال حدوث حوادث سيبرانية محتملة؛ ٣) الإجراءات الوقائية للحد من المخاطر السيبرانية؛ ٤) المخاطر السيبرانية لطبيعة الأعمال التجارية أو التشغيلية للشركات؛ ٥) تكاليف الحماية من المخاطر السيبرانية مثل التغطية التأمينية؛ ٦) الإضرار بالسمعة؛ ٧) التكاليف المتعلقة بالتنظيم الحالي أو المحتمل الجديد؛ و٨) مخاطر التقاضي)، ويجب على المنشآت تجنب استخدام اللغة المعيارية في الإفصاح المتعلق بالأمن السيبراني، وتقديم معلومات محددة مفيدة للمستثمرين)(SEC, 2018). وتوقعت (SEC) من المنشآت أن تصمم إفصاحاتها بما يتناسب مع المخاطر السيبرانية الخاصة بها، وقد يتم الإفصاح عن المخاطر السيبرانية في أقسام من ملفات(10-K)، مثل عوامل الخطر للبند(A1)، والبند (MD&A7)، والبند(A8)البيانات المالية والبيانات التكميلية، و البند(A9)الضوابط والإجراءات، وعلى سبيل المثال، وأوصت بأن تعالج المنشآت المخاطر السيبرانية في(MD&A)إذا كان من المحتمل أن يكون لها تأثير جوهري على نتائج العمليات أو السيولة أو الوضع المالي أو ستغير النتائج المالية المستقبلية. ويوضح **الجدول رقم (٢)** الاختلافات بين إرشادات لجنة الأوراق المالية الأمريكية لعام ٢٠١١ وبيان ٢٠١٨كالتالي:

١ - IOSCO هو المنتدى الدولي الراعي للسياسات لمنظمي الأوراق المالية وهو معترف به باعتباره واضع المعايير العالمية لتنظيم الأوراق المالية، وتنظم عضوية المنظمة أكثر من ٩٥٪ من أسواق الأوراق المالية العالمية في أكثر من ١١٥ دولة، ويعتبر مجلس إدارة المنظمة هو الهيئة الحاكمة ووضع المعايير، وتعد البورصة المصرية من أعضاء مجلس الإدارة.

الجدول رقم (٢)
الاختلافات بين إرشادات لجنة الأوراق المالية الأمريكية لعام ٢٠١١ وبيان ٢٠١٨

	بيان ٢٠١١	إرشادات ٢٠١٨
التسلسل الهرمي للنشر	يمثل منشور ٢٠١١ رأي فريق(SEC)وهو يقدم أول توجيه شامل حول كيفية تعامل المؤسسات العامة مع المخاطر السيبرانية.	تتبنى(SEC)رسمياً البيان الخاص بإفصاحات المخاطر السيبرانية، وهو يمثل الموقف الرسمي للجنة بشأن ماذا وكيف تفصح المنظمات العامة عن مخاطر وحوادث الأمن السيبراني.
وصف مشهد الهجوم السيبراني	يركز على الهجمات أو الانتهاكات المتعمدة أو غير المقصودة التي تهدف إلى تعطيل العمليات التجارية أو محاولة سرقة البيانات.	بالإضافة إلى منشور ٢٠١١، يمكن للمهاجمين إشراك الدول القومية، لا يقتصر الهجوم على الوصول غير المصرح به أو سرقة البيانات، بهدف تعطيل العمليات؛ ويمكن أن تهدف إلى تدمير البنية التحتية.
ضوابط وإجراءات الإفصاح	يجب أن تكون ضوابط وإجراءات الإفصاح جزءاً من تقييمات الرقابة الداخلية، لتقييم كيفية تأثير المخاطر السيبرانية على قدرات المنشآت على تسجيل المعلومات ومعالجتها وتلخيصها والإبلاغ عنها.	تعمل ضوابط وإجراءات الإفصاح كجزء من آلية حوكمة المنشآت، وأن تتأكد المنظمات من تحديد سلسلة إبلاغ واضحة واستخدامها في حالة حدوث خرق، وأن لدى كبار المديرين القدر المناسب من المعلومات لاتخاذ قرارات تحديد الأهمية النسبية والإفصاح، ويجب توثيق كيفية مشاركة مجلس الإدارة في حوكمة إدارة المخاطر السيبرانية.
موقع الإفصاح	يتم الإفصاح عادةً في خمسة أقسام من التقارير الدورية:(عوامل الخطر، ومناقشة الإدارة، ووصف الأعمال، والإجراءات القانونية، والبيانات المالية).	بالإضافة إلى التقارير الدورية، يُطلب من المنظمات استخدام تقرير حالي، مثل النموذج(K-10)، لتحسين توقيت الإفصاح عن حوادث الأمن السيبراني.
التداول من الداخل	لم يتم مناقشته.	يجب على المنشآت تنفيذ سياسات بشأن التداول من الداخل أثناء وبعد حوادث الأمن السيبراني.
ضوابط وإجراءات إدارة المخاطر السيبرانية	لم يتم مناقشته.	يمكن الإبلاغ عن الاستنتاجات المتعلقة بفعالية ضوابط وإجراءات الإفصاح في البند (A9) (الضوابط والإجراءات).
إشراف مجلس الإدارة على المخاطر السيبرانية	لم يتم مناقشته.	الإفصاح عن سياسات وإجراءات الأمن السيبراني لتحديد وإدارة المخاطر السيبرانية ودور الإدارة في تقييم المخاطر السيبرانية وتحليلها وتنفيذ السياسات وإجراءات الأمن السيبراني، واقترح تقارير سنوية الزامية، في النموذج(K-10) أو النموذج(F-20)لتوفير تحديثات بشأن أي تغييرات جوهرية لحوادث الأمن السيبراني المبلغ عنها في النموذج(K-10). يجب على المنشآت النظر فيما إذا كان مجلس إدارتها بصيغته الحالية، يتمتع بعمق كافٍ من الخبرة في مجال الأمن السيبراني فيما يتعلق بتهديد حوادث الأمن السيبراني لعملياتهم ووضعهم المالي.

المصدر: بتصرف الباحث، اعتماداً على الدراسات السابقة.

وفي ١١مارس٢٠٢٢، أصدرت (SEC)تعديلات لتعزيز وتوحيد متطلبات الإفصاح الالكتروني المتعلقة بإدارة الأمن السيبراني، والإبلاغ عن الحوادث السيبرانية والتقارير الدورية من قبل المنشآت لإعلام المستثمرين بشكل أفضل بإدارة مخاطر المنشأة واستراتيجيتها وحوكمتها المتعلقة بالمسائل الإلكترونية، وتقديم إخطار في الوقت المناسب بحوادث الأمن السيبراني الجوهرية، وبموجب القواعد المقترحة يُطلب من المنشآت العامة ما يلي:(الإبلاغ عن حادثة جوهرية للأمن السيبراني في غضون أربعة أيام عمل في النموذج(K-8) أو النموذج(K-6) الإفصاح عن سياسات وإجراءات الأمن السيبراني لتحديد وإدارة المخاطر السيبرانية ودور الإدارة في تقييم المخاطر السيبرانية وتحليلها، واقترح تقارير سنوية الزامية، في النموذج(K-10) أو النموذج(F-20)- توفير تحديثات بشأن أي تغييرات جوهرية لحوادث الأمن السيبراني المبلغ عنها في النموذج(K-10) والنموذج(Q-10) أوالنموذج(F-20)، والإفصاح في تعليقات الإدارة عن أي خبرة في مجال الأمن السيبراني لمجلس إدارتها، فضلاً عن تقديم إفصاحات الأمن السيبراني بلغة تقارير الأعمال الموسعة في Inline XBRL للوصول إليها بسهولة، وأرفقت(SEC) هذه الافصاحات بقاعدة تشريعية قانونية متمثلة بقانون الأوراق لمخاطر وحوادث الأمن السيبراني الأمريكي(akingump ,2022,p1; Trautman and Newman, 2022, p7).

٢/٣/٤- إرشادات لجنة الأوراق المالية الكندية(CSA): سيراً على خطى هيئة الأوراق المالية والبورصات، نشرت لجنة الأوراق المالية الكندية إشعار فريق العمل رقم(326–11)الأمن السيبراني في عام ٢٠١٣ والذي حدد تحديات الجريمة السيبرانية، وفي عام ٢٠١٦ أصدرت إشعار فريق العمل رقم(332–11)لتسليط الضوء على حجم وأهمية المخاطر السيبرانية للمصدرين والمسجلين والكيانات الخاضعة للتنظيم وإبلاغ أصحاب المصلحة، وتحليل ما يتم الإفصاح عنه فيما يتعلق بالمخاطر السيبرانية والهجمات السيبرانية، ما إذا كان المنشآت قد عالجوا قضايا الأمن السيبراني، وما إذا كان الإفصاح قد وصف الآثار المحتملة للهجوم السيبراني، ونوع المعلومات الجوهرية التي يمكن الإفصاح عنها، والإفصاح عن أي حوادث أمنية إلكترونية سابقة(Héroux and Fortin, 2020, p80). وقدمت بورصة بورصة تورنتو(TSX)مؤشراً للإفصاح عن المخاطر السيبرانية من أربعين فقرة موزعة في **سبع فئات** يتكون من عدة أبعاد منها:(إشراف مجلس الادارة، ومستوى مجلس الادارة، واعداد تقارير الادارة، والابلاغ عن ادارة المخاطر السيبرانية، وجهود الادارة لتخفيض المخاطر السيبراني، والتعليم والتدريب)(يعقوب وآخرون, ٢٠٢٢، ص ١٤١٢).

٣/٤- تحليل الجهود المصرية ومبادرة البنك المركزي المصري في دعم الأمن السيبراني

عندما ننظر إلي رؤية جمهورية مصر العربية ٢٠٣٠ ، والتي تؤكد من خلالها علي أهمية التوسع في الاستخدام الإلكتروني في الأعمال الحكومية والعلمية والتجارية، فقد أشارت كثير من التقارير العالمية والمحلية إلي تعرض مصر إلى العديد من الهجمات السيبرانية، ولكن تم اتخاذ اجراءات الأمان والتحصين وبحسب ما أعلنت عنه إحدى المنشآت الأمنية السيبيرية الفرنسية، فإن هذا الهجوم يشل عمل الأجهزة الالكترونية ويستغل ثغرة موجودة في نظام تشغيل ويندوز" (البغدادي، ٢٠٢١، ص١٥٠٣).

١/٣/٤- تحليل الجهود المصرية في دعم الأمن السيبراني في ضوء رؤية مصر ٢٠٣٠: بخصوص الجهود المصرية في دعم والتصدي لمخاطر الأمن السيراني يتضح ما يلي: (الرشيدي، عباس، ٢٠١٩، ص٤٦٤-٤٦٦؛ البغدادي، ٢٠٢١، ص١٥٠٣-١٥٠٤؛ الفقي، ٢٠٢١، ص٢٢؛ يوسف، ٢٠٢٢، ص٣٣-٣٤؛ محروس, وأبو الحمد، ٢٠٢٢، ص ٤٥١-٤٥٢؛ على، على، ٢٠٢٢، ص٦؛ فرج, ٢٠٢٢، ص١٤٢-١٤٤؛ يعقوب وآخرون, ٢٠٢٢، ص ١٤١٢):

قد نص الدستور المصرى عام ٢٠١٤ (م ٣١) على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الإقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"؛ثم صدر قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧ بإلزام كافة الجهات الحكومية بتنفيذ قرارات المجلس الأعلى للأمن السيبراني بشأن تأمين البنية التحتية للإتصالات وتكنولوجيا المعلومات. وتلى ذلك إصدار الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧- ٢٠٢١)، والتي تضمنت أهم **التحديات والأخطار السيبرانية** والتي تتمثل في خطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات، وخطر الإرهاب والحرب السيبرانية، وخطر سرقة الهوية الرقمية والبيانات الخاصة، وأهم **القطاعات الحيوية المستهدفة**، وتشمل بالترتيب قطاع الاتصالات وتكنولوجيا المعلومات، قطاع الخدمات المالية، قطاع الطاقة، وقطاع الخدمات الحكومية، قطاع النقل والمواصلات، وقطاع الاعلام والثقافة، وعناصر التهديدات السيبرانية، وركائز التوجه الإستراتيجي للخطر السيبراني، وآلية تنفيذ الإستراتيجية، وهدفت إلى مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية التحتية للإتصالات والمعلومات وتطبيقاتها وخدماتها من أجل التنمية الشاملة وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثقة للمجتمع المصري. ثم صدر القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، لدعم منظومة مواجهة المخاطر السيبرانية، ثم صدر قرار رئيس الوزراء رقم ٢٧٦ سنة ٢٠٢٠ الخاص بتعيين رئيس المكتب التنفيذي للمجلس الأعلى للأمن السيبراني ورئيس الأمانة الفنية.

٢/٣/٤- مبادرات وتعليمات البنك المركزي المصري في دعم الأمن السيبراني: في نفس السياق قام **البنك المركزي المصري** بإنشاء مركز الاستجابة لطوارئ الحاسب الآلي بهدف توفير الحماية اللازمة للمتعاملين مع البنوك وتعزيز الأمن السيبراني في القطاع المصرفي، ويقوم هذا المركز بالتعامل والإبلاغ الفوري عن أي مخاطر سيبرانية وتعميم الإنذار المبكر والتنبيهات واتخاذ الإجراءات الاحترازية، والقيام أيضا بالمراقبة الأمنية وتحديد التهديدات الالكترونية المحتملة، وفحص وتقييم المخاطر المرتبطة بالثغرات الأمنية والبرمجيات الضارة (صندوق النقد العربي، ٢٠١٩). كما أطلق البنك المركزي مبادرة تعزيز الأمن

السيبراني في القطاع المصرفي، والتي تهدف إلى زيادة أعداد الخبراء المعتمدين دوليا في مجال الأمن السيبراني في القطاع المصرفي (البنك المركزي المصري، ٢٠١٩). وبالرغم من ذلك يرى (الرشيدي وعباس، ٢٠١٩) أنه في بيئة الأعمال المصرية هناك ضعف في الإفصاح عن المخاطر السيبرانية وبرامج إداره مخاطره في القطاع المالي، كذلك ليس هناك أي إرشادات للشركات المصرية المسجلة تدعم المنشآت في الإفصاح عن المخاطر السيبرانية وإدارة مخاطره، حيث تعتبر الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١) عامة و غير موجهه.

وفي ضوء **تعليمات البنك المركزي** فيما يتعلق **بتكنولوجيا المعلومات والاتصالات والأمن السيبراني،** أنه يجب على البنك التأكد من قوة نظم تكنولوجيا المعلومات والاتصالات والأمن السبراني لديه وأن تكون خاضعة لبرامج الحماية وإصلاح أي خلل، وأن يتم اختبارها بشكل دوري ومنتظم للتأكد من توفير المعلومات لمستخدميها في الوقت المناسب من أجل تقديم الدعم وتسهيل أداء عمليات البنك الاساسية والحيوية(البنك المركزي المصري، ٢٠٢١، ص٨). ويلتزم البنك بالإقرار سنوياً للبنك المركزي المصري عن أحداث الخسائر الفعلية المتعلقة بمخاطر التشغيل وفقاً لمصفوفة تجميع بيانات الخسائر كما هو موضح بالجدول التالي رقم(٣)، ووفقاً للتعريفات والأمثلة الإيضاحية الواردة بالجدول التالي رقم(٤)، ويلتزم البنك بالإبلاغ بشكل تفصيلي لأحداث خسائر التشغيل التي تبلغ مليون جنيه مصري فأكثر، ويشمل ذلك شرح تفصيلي للحدث وأسبابه والإجراءات التصحيحية التي قام البنك باتخاذها كما هو موضح بالجدول التالي رقم(٥). وبالإضافة إلى المعلومات المتعلقة **بإجمالي مبالغ الخسائر المحققة،** يجب على البنك أن يجمع معلومات عن التواريخ المرتبطة بأحداث مخاطر التشغيل كما يلي(البنك المركزي المصري، ٢٠٢١، ص١٥):(**تاريخ اكتشاف الحدث**: وهو تاريخ بدء الحدث أو التاريخ الذي أصبح فيه البنك على علم بالحدث، **وتاريخ الخسارة:** يمثل التاريخ (أو (التواريخ التي تحققت فيها خسارة فعلية نتيجة هذا الحدث، و**تاريخ إثبات الخسائر محاسبياً**: هو التاريخ الذي تم فيه تسجيل الخسائر ضمن حساب الأرباح والخسائر. وبالإضافة إلى ماتقدم، يجب على البنك تجميع المعلومات المتعلقة بأي مبالغ مستردة من إجمالي الخسائر -إن وجدت-، وكذلك أي معلومات تفصيلية تتعلق بالأسباب التي أدت إلى حدوث الخسارة، ويجب أن يكون مستوى التفاصيل لأي معلومة يتناسب مع حجم الخسارة.

الجدول رقم (٣)

مصفوفة تجميع بيانات الخسائر

البيان		وسائل احتيال داخلية	وسائل احتيال خارجية	الاحتيال على بطاقات الائتمان	الممارسات الخاطئة في حق عملاء البنك	الإضرار بالأصول المادية للبنك	تعطل العمل وإخفاق النظام	القصور في إدارة وتنفيذ العمليات	إجمالي أنواع الأحداث
		١	٢	٣	٤	٥	٦	٧	
إجمالي الأنشطة	عدد الأحداث	××	××	××	××	××	××	××	××
	أعلى خسارة	××	××	××	××	××	××	××	××
إجمالي قيمة الخسائر			××	××	××	××	××	××	××
الاستردادات	استردادات تأمينية	××	××	××	××	××	××	××	××
	استردادات أخرى	××	××	××	××	××	××	××	××
صافي قيمة الخسارة		××	××	××	××	××	××	××	××

المصدر: البنك المركزي المصري، ٢٠٢١، صـ٢٠.

- **تجميع بيانات الخسائر المتعلقة بمخاطر التشغيل**

يجب على جميع البنوك تصنيف الخسائر الفعلية الناتجة عن مخاطر التشغيل وفقاً لنتائج الأحداث التالية، وفي ضوء الجدول الاسترشادى التالي **رقم (٤)**، ويتضمن مايلي:(وسائل احتيال داخلية، وسائل احتيال خارجية، ووسائل احتيال على بطاقات الائتمان، والممارسات الخاطئة في حق عملاء البنك، والاضرار بالأصول المادية للبنك، وتعطل العمل وإخفاق النظام، والقصور في إدارة وتنفيذ العمليات)(البنك المركزي المصري، ٢٠٢١، ص٥-٦).

الجدول رقم (٤)
مستويات التعريف التفصيلية لأنواع الأحداث المسببة للخسائر

م	نوع الحدث (المستوى الأول)	التعريف	الأقسام (المستوى الثاني)	أمثلة إيضاحية (المستوى الثالث)
١	وسائل احتيال داخلية	خسائر تنتج عن أفعال يقصد بها التزوير واختلاس الممتلكات أو التحايل على اللوائح أو سياسات البنك.	أفعال غير مسموح/ مصرح بها.	- عمليات لم يتم الإخطار عنها (عمداً). - عمليات غير مصرح بها تتسبب في حدوث خسائر مادية. - إظهار المراكز المالية بصورة خطأ (عمداً). -
			السرقة والاحتيال	- الاحتيال/ السرقة الابتزاز/ النصب والاختلاس. - الإتلاف العمدي للأصول - تهريب الأموال، والاستيلاء على حسابات العملاء - إجراء عمليات التداول الداخلي لغير صالح البنك.
٢	وسائل احتيال خارجية	خسائر تنتج عن أفعال بغرض الاحتيال بدون حق من طرف ثالث.	السرقة والاحتيال	- السرقة، التزوير، سرقة الشيكات.
			أمن النظام	- التلف الناشئ عن التسلل للنظام. - سرقة المعلومات الناتج عنها خسائر مادية.
٣	وسائل احتيال على بطاقات الائتمان	تنتج عن أفعال بغرض الاحتيال والسرقة(داخلياً أو خارجياً).	-------	-------
٤	الممارسات الخاطئة في حق عملاء البنك	خسائر تنتج عن إخفاق غير مقصود أو الإهمال في الوفاء بالالتزام المهني تجاه عملاء معينين (بما في ذلك متطلبات الثقة والكفاءة).	أمور متعلقة بالثقة والإفصاح والكفاءة	- مخالفات ائتمانية/ مخالفة التعليمات المتعلقة بالإفصاح والكفاءة(اعرف عميلك... الخ. - انتهاك سرية المعلومات. - إجراء العديد من المعاملات على حساب العميل لتحقيق عمولات أكثر. - إساءة استخدام المعلومات السرية.
			ممارسات غير سليمة	- معاملات غير مسموح بها قانونياً. - إجراء التداول الداخلي على حساب العملاء. - نشاطات غير مرخص بها/ غسل الأموال.
			عيوب/ مشاكل في تقديم المنتجات/ الخدمات	- وجود خلل في المنتجات والخدمات المقدمة للعملاء - الفشل في الاستعلام عن العملاء وفقاً للشروط.
٥	الإضرار بالأصول المادية للبنك	خسائر ناشئة عن ضياع أو تلف الأصول المادية نتيجة الكوارث الطبيعية أو أحداث أخرى(بما في ذلك المخاطر السيبرانية).	الكوارث الطبيعية أو أحداث أخرى(بما في ذلك المخاطر السيبرانية).	- خسائر نتيجة كوارث طبيعية. - خسائر نتيجة التعرض لهجمات سيبرانية.
٦	تعطل العمل وإخفاق النظام	خسائر ناشئة عن اضطراب النظم العمل أو فشل النظام.	نظم العمل	- تعطل الأجهزة والبرامج الالكترونية ووسائل الاتصال - انقطاع الخدمة /اختلال العمل.
٧	القصور في إدارة وتنفيذ العمليات	خسائر تنتج عن الفشل في إدارة العمليات، أو نتيجة العلاقات مع الأطراف الأخرى في التداول والعمليات.	تخطيط وتنفيذ المعاملات	- سوء عملية الاتصال، أخطاء في إدخال البيانات. - عدم الالتزام بالمواعيد النهائية أو المسؤوليات. - تشغيل النظام بشكل خاطئ، وأخطاء محاسبية. - الفشل في تسليم الخدمات، وإدارة الضمانات.
			الرقابة والتقارير الرقابية	- عدم الالتزام بتقديم التقارير الإلزامية. - عدم دقة التقارير الخارجية عن الخسائر المحققة.
			إدارة حسابات العملاء	- عدم الحصول على موافقة العميل للاطلاع على الحسابات. - عدم صحة سجلات العملاء (الخسائر المحققة) - خسائر الإهمال أو التلف الأصول خاصة بالعملاء.

المصدر: البنك المركزي المصري، ٢٠٢١، صـ٢١-٢٣.

الجدول رقم (٥)
أحداث التشغيل التي تبلغ قيمتها ١ مليون جنيه فأكثر

نوع الحدث	تاريخ الاكتشاف	القيمة(بالألف جنيه)	الوصف التفصيلي للحدث	الإجراءات التصحيحية
وسائل احتيال داخلية				
وسائل احتيال خارجية				
وسائل احتيال على بطاقات الائتمان				
الممارسات الخاطئة في حق العملاء				
الإضرار بالأصول المادية للبنك				
تعطل العمل وإخفاق النظام				
القصور في إدارة وتنفيذ العمليات				

المصدر: البنك المركزي المصري، ٢٠٢١، صـ٢٤.

وفي ضوء **تعليمات البنك المركزي** يتعين على البنك **ادارة الحوادث**، وذلك من خلال وضع وتطوير وتنفيذ خطط التعافي من الحوادث التي يمكن ان تعطل تنفيذ الاعمال الاساسية والحيوية لديه، ويجب أن تتماشى هذه الخطط مع قدرته على تحمل المخاطر والإطار العام للمخاطر لديها، كما يجب أن تقوم بتطوير هذه الخطط بشكل مستمر بناءً على الدروس المستفادة من الحوادث السابقة (البنك المركزي المصري، ٢٠٢١، ص٨).

وفيما يتعلق بخطط التعافي من الكوارث والمخاطر التشغيلية الناشئة، يتعين إدراج المؤشرات الكمية والنوعية التالية ضمن خطة التعافي كحد أدنى، مع ضرورة إدراج القيم الفعلية للمؤشرات الكمية وفقاً لآخر قيمة / مركز متاح قبل تاريخ اعتماد الخطة، وتشمل **المؤشرات الكمية**(مؤشرات رأس المال، ومؤشرات السيولة والربحية، مؤشرات السوق والاقتصاد الكلي)، وتشمل **المؤشرات النوعية**-على سبيل المثال وليس الحصر- (المخاطر الناشئة عن الاسترداد المبكر لمصادر التمويل، بالإضافة إلى المخاطر الاستراتيجية **والمخاطر السيبرانية**، وأية مخاطر أخرى قد تنشأ عن مخالفة المتطلبات القانونية أو الرقابية، أو الدعاوى القضائية المقامة ضد البنك) (البنك المركزي المصري، تعليمات خطط التعافي، ٢٠٢١، ص٥-٦).

ويتعين على البنوك وضع **سيناريوهات** لخطة التعافي تتماشى مع نموذج أعمال البنك، وحجم أنشطته، ومدى تعقد عملياته المصرفية، والمخاطر التي يتعرض لها، ومستوى الملاءة المالية والسيولة لديه، وتلتزم البنوك بإعداد سيناريو واحد كحد أدنى، مثل؛ سيناريو للضغوط على مستوى البنك أو المجموعة المصرفية - Idiosyncratic Stress Scenario على سبيل المثال لا الحصر: تحقيق خسائر تشغيلية كبيرة، أو خسائر نتيجة لنزاعات قضائية، أو تعرض البنك للاحتيال أو لهجمات سيبرانية أو لأزمة تضر بسمعته) (البنك المركزي المصري، تعليمات خطط التعافي، ٢٠٢١، ص٨-٩). ويجب على مجلس الإدارة والإدارة العليا الإشراف على التطوير والصيانة المستمرة للبنية التحتية للرقابة الأمنية التي توفر الحماية المناسبة لنظم وبيانات خدمات الإنترنت البنكي من أي تهديدات داخلية أو خارجية، ومن أجل ضمان فعالية عملية تأمين خدمات الإنترنت البنكي، يجب على مجلس الإدارة والإدارة العليا التأكد من اتخاذ الإجراءات الآتية(البنك المركزي المصري، ٢٠١٩، ص٥-٦) :

- تحديد مسئوليات واضحة خاصة بالإشراف على وضع وإدارة السياسات الأمنية الخاصة بالبنك.
- توفير الحماية اللازمة لمنع دخول غير المصرح لهم إلى بيئة الحاسب الآلي، والتي تتضمن كافة الأنظمة الحيوية وقواعد البيانات والتطبيقات والاتصالات، والأنظمة الأمنية الخاصة بخدمات الإنترنت البنكي.
- توفير الضوابط الإلكترونية اللازمة والتي من شأنها منع أي أطراف داخلية أو خارجية غير مصرح لها من الوصول إلى التطبيقات وقواعد البيانات الخاصة بخدمات الإنترنت البنكي.

- المراجعة الدورية لعمليات اختبار الإجراءات والنظم الأمنية (على سبيل المثال إجراء اختبار الاختراق دورياً، بما في ذلك المتابعة المستمرة للتطورات في النظم الأمنية في هذا المجال، وتحميل وإعداد التحديثات الخاصة بالبرامج وحزم الخدمات والتدابير اللازمة وذلك بعد إجراء الاختبارات المطلوبة.

وفيما يتعلق بتقييم النظام الأمني، يجب علي البنوك دورياً تقييم الوضع الأمني لكافة الأنظمة التطبيقات، والشبكات، وأجهزة التأمين، وخوادم نظام أسماء النطاقات وخوادم البريد الإلكتروني، إلخ) المتعلقة بأعمال الإنترنت البنكي، وذلك في المركز الرئيسي للمعلومات والمركز الاحتياطي الذى يستخدم في حالات الكوارث، ويجب على البنوك إجراء تقييم دوري لنقاط الضعف Vulnerability Assessment كل ثلاثة أشهر على الأقل أو عند حدوث تغييراً جوهرياً في البيئة التشغيلية لنظام خدمات الإنترنت البنكي، لاكتشاف نقاط الضعف في بيئة تكنولوجيا المعلومات وتقييمها(البنك المركزي المصري، ٢٠١٩، ص١٩). ويجب على البنك القيام **باختبارات الاختراق** Penetration Testing وذلك لعمل تقييم مفصل ومتعمق للوضع الأمني للنظام من خلال محاكاة للهجمات الفعلية على النظام على أن يتم ذلك على الأقل مرة واحدة سنوياً، أو قبل البدء في تقديم أي خدمات حيوية جديدة، على أن تتم مراعاة ما يلي(البنك المركزي المصري، ٢٠١٩، ص١٩-٢٠):

- يجب أن يتولى إجراء اختبار الاختراق أحد مقدمي الخدمة الخارجيين المستقلين، حيث يجب عليه أولاً التوقيع على اتفاقية السرية وعدم الإفصاح قبل مزاولة العمل، وغير مسموح باختيار نفس مقدم الخدمة الخارجي لأداء أكثر من اختباري اختراق متتاليين.
- يجب أن يكون لدى البنوك تقرير مبدئي عن اختبار الاختراق وخطة المعالجة، التي تم اصدارها وموقعة.
- يجب علي البنوك التحقق من صحة معالجة الملاحظات الناتجة عن اختبار الاختراق سواء كان علي الأنظمة الرئيسية أو الأنظمة البديلة المستخدمة لمواجهة الكوارث.
- يجب على مقدم الخدمة الخارجي إصدار تقرير نهائي موقع منه عن اختبار الاختراق لكي يقوم البنك بتقديمه إلى البنك المركزي المصري، بجانب التقرير المبدئي الأول.

وفيما يتعلق بالاستجابة للأحداث وإدارتها، يجب علي البنوك وضع إجراءات للاستجابة للحدث وإدارته خلال تقديم الخدمة، بهدف الإبلاغ والمعالجة الفورية لأي اختراقات أمنية، وكذلك أي حالات احتيال أو انقطاع/عدم ثبات الخدمة في الأنظمة الخاصة بخدمات الإنترنت البنكي، ويجب علي البنوك اتخاذ الإجراءات الضرورية التالية: (سرعة اكتشاف مصدر الحدث، وتقييم النطاق المحتمل للحدث ومدي تأثيره، وتصعيد الأمر إلى الإدارة العليا للبنك بشكل فورى، وما إذا كان هذا الحدث قد يضر بسمعة البنك أو يؤدى إلى خسائر مالية، وإخطار العملاء المتضررين على الفور، واحتواء الخسائر المتعلقة بأصول البنوك وبياناته وسمعته، وبوجه خاص الخسائر المتعلقة بعملائها الأدلة الجنائية وحفظها بطريقة مناسبة وبأسلوب يضمن الرقابة على تلك الأدلة، بالإضافة إلى تنفيذ عملية مراجعة لهذا الحدث)، وعند وقوع هجمات إلكترونية، يمكن أن يؤخذ في الإعتبار من ضمن التدابير التي يتبناها البنك التواصل مع فريق التدخل السريع لمكافحة الجرائم الإلكترونية EGYPTIAN-CERT التابع لوزارة الاتصالات(البنك المركزي المصري، ٢٠١٩، ص٢٠).

ويخلص الباحث، أنه في مصر، يتضح عدم وجود تقنين للإفصاح عن المخاطر السيبرانية، ولا توجد أية معايير محاسبية أو مصرية –حتى الآن- تناولت ذلك الإفصاح بصورة مباشرة، وأنه ما زال الإفصاح في مصر اختيارياً، وإن حدث سيكون ضمن الإيضاحات المتممة، كما لا توجد أية متطلبات من سوق الأوراق المالية المصرية للشركات المقيدة بالبورصة بتقديم مثل هذا النوع من الإفصاح، وأن إصدار قانون ملزم للشركات المقيدة بالبورصة للإفصاح عن المخاطر السيبرانية وبرامج إدارتها، أصبحت ضرورة ملحة في الوقت الراهن، خاصةً وأن مصر تتعرض لهجمات سيبرانية مرتفعة في الوقت الحالي.

خامساً: قيمة المنشأة من منظور محاسبي(بين المفهوم ومداخل القياس)

١/٥- مفهوم وأهمية قياس قيمة المنشأة من المنظور المحاسبي

لقد اهتم الفكر المحاسبي بتحديد قيمة المنشأة، وخاصة بعدما تغير الهدف الذي تسعي إلي تحقيقه الإدارة من العمل علي تعظيم ربحية المنشأة إلي العمل علي تعظيم قيمتها(Islam et al., 2022, p14). وفي الأسواق الفعالة، يجب أن يعكس رد الفعل العائد على الهجوم السيبراني والضرر الذي يلحق بالمنشأة من جراء الهجوم، ولكن في حالات حجب المعلومات، يجب أن يعكس أيضاً السمعة السلبية المرتبطة بحجب المعلومات؛ وقد يستنتج المستثمرون من المنشآت التي لديها معلومات عن هجوم سيبراني، أن الإدارة ليست صريحة تماماً بشأن المشاكل المحتملة الأخرى(Amir et al., 2018, p1191) .

وتتحدد قيمة المنشأة بالقيمة السوقية لأسهمها، وتمثل مقدار التدفقات النقدية المستقبلية المتوقعة على الأسهم، ولتحديدها **أهمية** كبيرة، تنعكس على كل من **المستثمرين** لأنها تعد انعكاساً لربحيتها الحالية وأرباحها الموزعة مستقبلاً، و**الدائنون** لأنها مؤشر على حجم السيولة لدي المنشأة وقدرتها على سداد قروضها، و**للإدارة** لما يترتب عليها من قرارات حالية ومستقبلية، حيث أن قيمة المنشأة تعني تدعيم لقدرتها التنافسية في السوق، وجذب المزيد من المستثمرين، مما يزيد من أسعار أسهمها(كريمة، ٢٠٢٣، ص٩٩١). وتكون قيمة المنشأة أقل مع المخاطر السيبرانية بسبب القيمة الحالية لمجموع التكاليف التي تتحملها المنشأة من الهجمات، واستثمارات إدارة المخاطر للتخفيف من الهجمات المستقبلية، والتعويضات التي يطلبها أصحاب المصلحة مقابل تعرضهم للمخاطر السيبرانية(Kamiya et al., 2021, p724).

وبناءً **على ما سبق، يستخلص الباحث أن قيمة المنشأة في البيئة الرقمية تعبر عن القيمة الحقيقية الفعلية للأصول في السوق، ومدى قدرة إدارة المنشأة في خلق منافع اقتصادية مستقبلية تساوي أو أكبر مما هو متوقع، من خلال الاستغلال الأمثل للموارد والفرص المتاحة في الأجلين القصير والطويل، وحماية أصولها من أي مخاطر وتهديدات سيبرانية حالية أو متوقعة في الفضاء السيبراني المحيط بالمنشأة، ووضع سيناريوهات واجراءات واضحة للتعامل مع أي أزمة أو ظروف طارئة قد تحدث بمرور الزمن.**

٢/٥- المداخل المحاسبية والسوقية لقياس قيمة المنشأة

يمكن قياس قيمة المنشأة بطرق مختلفة، فقد تستخدم مقاييس تعتمد على المعلومات المحاسبية فقط أو تعتمد على المعلومات المحاسبية والسوقية معاً، وسيتم **تناول مدخل الجمع بين الأرقام المحاسبية والسوقية(مقياس Tobin's Q)**. نتيجة للانتقادات الموجهة لمداخل قياس قيمة المنشأة استناداً للأرقام المحاسبية أو الأرقام السوقية، فقد أشارت العديد من الدراسات السابقة(أحمد، ٢٠١٩، ص١١٤؛ السيد وآخرون، ٢٠٢٠، ص٩٤٠-٩٤١؛ بيومي, ٢٠٢١، ص١٣٦١؛ صالح، وعلى، ٢٠٢١، ص٣٠؛ عفيفي، ٢٠٢١، ص٢١٥؛ كريمة، ٢٠٢٣، ص٩٩١-٩٩٢؛ Amir et al., 2018, p513; Smith et al., 2019; Juma'h and Alnsour, 2021; Benaroch, 2021; Tosun, 2021; Kamiya et al. 2021, p729 ; Islam et al., 2022, p19; Hussein & Nounou, 2022, p848; Ali et al., 2022; Masuch et al., 2022 ; Gatzert and Schubert, 2022, p725; Florackis et al., 2023, p403;)إلى ضرورة الجمع بين المدخلين كأساس للتقييم، لضمان الاستفادة من مزايا كل منهما، ومن أهم المقاييس التي عرفها الفكر المحاسبي لقياس قيمة المنشآت نسبة(Tobin's Q). وهذه النسبة مأخوذة من النموذج الذي قدمه عالم الاقتصاد جميس توبين الحائز على جائزة نوبل كنموذج لقياس الأداء(Mikial et al., 2020; Hapsoro and Bahantwelu, 2020; Paputungan et al.,2020)

.

وقد أشار(Dakhlallh et al., 2020) إلى أن هذا المقياس يعد أداة فعالة لتقييم قيمة المنشأة، وذلك لأنه يقيم أداء المنشأة من منظور السوق على المدي الطويل، وبالتالي يعكس القيمة الحالية للتدفقات النقدية المستقبلية بناءً على المعلومات الحالية والمستقبلية. ويتم قياس هذا المتغير باستخدام نموذج(Tobin's Q) وهو مقياس للقيمة السوقية للمنشأة ويحسب قيمة المنشأة من خلال المعادلة الأتية:(القليطي، ٢٠١٩، ص ٤١؛ عازر، ٢٠٢٢، ص٥٦؛ (Frederica, 2019, p3; Hapsoro and Bahantwelu, 2020, p. 61; Kamiya et al. 2021, p729; Tosun et al. 2021, p2; ; Gatzert and Schubert, 2022, p733; Florackis et al., 2022, p403; :Bamiatzi et al., 2023, p15)

$$\text{Tobin's Q} = \frac{\text{القيمة السوقية لحقوق الملكية + القيمة الدفترية لإجمالى الإلتزامات}}{\text{القيمة الدفترية لإجمالى الأصول}}$$

و(Tobin's Q)هي القيمة السوقية للمنشأة(سعر السهم نهاية العام مضروباً في الأسهم العادية القائمة+ القيمة الدفترية للديون) على إجمالي الأصول(Tosun et al., 2021, p4; Gatzert and Schubert, 2022, p733). وإذا بلغت Tobin's, Q >١فإن هذا يعني ارتفاع قيمة المنشأة ، أما اذا كانت < ١فإن هذا يعني انخفاض قيمة المنشأة ومحدودية فرصها في النمو(عفيفي وآخرون، ٢٠٢١، ص٢١٥؛ الباز، ٢٠٢٢، ص٨٨؛ كريمة، ٢٠٢٣، ص٩٩١).

وسيعتمد الباحث على نموذج(Tobin's Q)لقياس قيمة المنشأة في الدراسة التطبيقية، لاعتماده على كل من الأرقام المحاسبية والسوقية معاً، ويتلافى الانتقادات الموجهة إلى كل منهما، كما يستند على جميع عناصر الديون ورأس المال كأساس للتقييم ومن أكثر المقاييس شيوعاً، بالإضافة إلى توافر البيانات المحاسبية اللازمة لتطبيق النموذج، وهو مقياس طويل الأجل ويتناسب مع قياس أثر الإفصاح عن المخاطر السيبرانية للمنشأة على قيمتها.

٣/٥- تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وقيمة المنشأة

إن مؤشر القيمة السوقية للشركات هو أحد المؤشرات لتقييم التغيير في ثقة المستثمرين، لذلك، تناولت العديد من الدراسات تأثير الانتهاكات الأمنية على القيمة السوقية(Tweneboah-Kodua, 2018). وتوصلت إلى نتائج مختلفة لقياس أثر الإفصاح عن المخاطر السيبرانية على القيمة السوقية للمنشأة. ويعد فحص سلوك سعر السهم أحد العوامل الوكيلة لثقة المستثمرين، لأنه يعكس التكاليف والمخاطر المستقبلية الحالية والمتوقعة المرتبطة بالمخاطر السيبرانية، من منظور المستثمر ولإدارة المنشأة المتأثرة لأن سعر السهم يعكس قيمة المنشأة، وتشير الزيادة (الانخفاض) في سعر السهم غالباً إلى زيادة (انخفاض) ثقة المستثمرين في التدفقات النقدية المستقبلية للمنشأة(Ali et al., 2021, p4). ويمكن أن تؤثر المخاطر السيبرانية على البيانات المالية، نظراً لأن هذه الآثار يجب أن تكون جزءاً من القياس الكمي للأثر الاقتصادي لها، ويجب قياس عوائد الأسهم على مدى جداول زمنية ممتدة تلي لإعلان (Ali and Lai, 2022, p692). وتؤثر الهجمات السيبرانية التي يتم الإفصاح عنها على أسعار الأسهم وأحجام التداول، ويتوقف هذا الأثر على عدة عوامل منها حجم الأصول المملوكة للمنشأة وقوة السوق المطروح فيه الأسهم؛ ونوع وحجم الخطر السيبراني التي تعرضت له المنشأة وتم الإفصاح عنه، ودرجة الشفافية التي تم عرض الخبر بها(الرشيدي، عباس، ٢٠١٩، ص ٤٤٤؛ يوسف، ٢٠٢٢، ص٣٥).

١/٣/٥- إنعكاسات الإفصاح عن المخاطر السيبرانية على قيمة المنشأة

يتوقع كل من السوق والمستثمرين زيادة في عمليات الإفصاح عن المخاطر السيبرانية ومعاقبة المنشآت المخترقة التي تقلل من الإفصاح عن المخاطر السيبرانية (Chen et al., 2022, p1). وشكلت العلاقة بين الإدارة والمساهمين تحديات كبيرة، نظراً لأن المخاطر السيبرانية يمكن أن يكون لها تأثير كبير على قيمة المنشأة لأصحاب المصلحة(Cortez, 2022, p3). وقد ينظر المشاركون في السوق إلى انتهاكات الأمن السيبراني التي تم الإفصاح عنها في ضوء إيجابي، لأنهم يقدرون حقيقة أن إدارة المنشأة على استعداد لإجراء هذا الإفصاح الطوعي(Janvrin and Wang, 2021, p8, 23). ويعتمد رد فعل السوق على التغيرات في الإفصاح بالزيادة أو الانخفاض عن المخاطر السيبرانية، وذلك على الرغم من عدم وجود رد فعل كبير في السوق إذا تضمنت التقارير السنوية زيادة في الإفصاح عن المخاطر السيبرانية، بينما إذا تضمن محتوى الإفصاحات المتزايدة تدابير إضافية لمنع المخاطر، فمن المحتمل أن يكون رد فعل السوق إيجابياً، ويحدث رد فعل سلبي كبير في السوق إذا قللت المنشآت المخترقة من الإفصاح عن المخاطر السيبرانية(Chen et al., 2022, p8-9). ويجب أن تكون المنشآت على دراية بالتآكل المحتمل في تقييمها، وأن تختار وتفصح بشكل استباقي التدابير المضادة المناسبة للتخفيف من المخاطر السيبرانية، ومن خلال القدرة على تحديد الأثر المالي المحتمل لإعلان الخرق(Viancourt, 2021,p89).

وتستجيب المنشأة التي تفصح عن المخاطر السيبرانية بشكل أفضل مقارنةً بشركة لم تفعل ذلك، ويقدم هذا دليلًا على الضوء الإيجابي على المخاطر النظامية المتعلقة بالأمن السيبراني بقدر ما يتم تحفيز السوق

والمنشأة نفسها على دمج هذه التأثيرات في أسعار الأصول، حيث أن تقييم الإدارة للمخاطر السيبرانية، يعزز قدرة المنشأة على الإستجابة وتقليل عدم تناسق المعلومات، ويجبر الإدارة على أن يكون لديها استراتيجيات طارئة، مما يؤدي إلى التقييم العادل لهذه المخاطر(Histen , 2022, p1, 3, 5, 11). وفي معظم الدراسات، لوحظ التأثير السلبي على القيمة السوقية تجلى في العوائد السلبية غير الطبيعية، واعتمدت هذه الدراسات على فرضية السوق شبه الفعالة، والتي بموجبها تتكيف أسعار الأسهم بسرعة مع جميع المعلومات الجديدة(Ali and Lai, 2022, p689-690). وتتأثر هذه العلاقة بنوع الخرق(متعلق بالوظيفة أو بالبيانات)، حيث أن الاختراقات الأمنية المتعلقة بالوظيفة(تعطل الخدمة) تؤثر سلبياً على عوائد الأسهم بشكل أكبر من الاختراقات المتعلقة بالبيانات(Ebrahimi and Eshghi, 2022, p18-19).

وتوصلت دراسة(Tong, 2023, p7, 10)إلى أن الهجمات السيبرانية لها تأثير سلبي قصير المدى على سعر سهم الشركة، وهو أمر ذو دلالة إحصائية عند مستوى ١٪، على الرغم من أن سعر سهم الشركة بشكل عام يتأثر أكثر بحجم الشركة، والعائد على الأصول ROA، والرافعة المالية ومؤشرات التشغيل التقليدية الأخرى للشركة، ولكن في العوائد التراكمية غير الطبيعية(CAR) بعد الهجوم الإلكتروني، يمكن أن يصل معامل الارتباط للهجوم الإلكتروني إلى -٠,٠١٣٩، ومستوى المعنوية(P-value) هي ٠,٠٠٣، وهي ذات دلالة إحصائية عند مستوى ١٪، ولذلك، يجب على الشركات اتخاذ تدابير وقائية ضد الهجمات السيبرانية ووقف الخسارة بشكل فعال بعد الهجمات، وأظهرت نتائج التحليل المقطعي أن الإفصاح الفعال عن معلومات الهجمات السيبرانية وتحسين درجة الإفصاح عنها يمكن أن يقلل التأثير السلبي للهجمات السيبرانية إلى حد معين.

وعندما يحتاج المستثمرون إلى تعويض أعلى عن حيازة الأسهم ذات التعرض العالي للمخاطر السيبرانية، وفقاً لذلك، يتوقع أن يكون هناك تفاوتات سلبية في عائدات الأسهم (Florackis et al., 2023, p351). ويتفاعل مستثمرو الأسهم بشكل سلبي مع الإعلانات عن انتهاكات البيانات، وبلغ متوسط (CAR) التراكمي نسبة ٠,٨٤ ٪ خلال فترة ثلاثة أيام، وبمتوسط قيمة سوقية تبلغ حوالي ٥٨,٩٣ مليون دولار، مما يؤثر سلبياً على القيمة السوقية للشركات المتضررة (Kamiya et al., 2021, p731). وتوصلت دراسة (Jeong et al., 2019) إلى انخفاض القيمة السوقية للشركات المخترقة بشكل كبير، وتحركت القيمة السوقية لمنافسيها في اتجاه معاكس. وأشارت دراسة(Dong et al., 2021,p18) إلى أن أحداث خرق البيانات في فترة ما بعد COVID تؤثر على أسعار أسهم المنشآت المخترقة بشكل سلبي أكثر مما كانت عليه في فترة ما قبل COVID. وفي الحالات التي حجبت فيها المنشآت المعلومات وكشفها المستثمرون كان رد فعل السوق سلبياً وهاماً(Amir et al., 2018, p1192) . وعندما تستجيب المنشأة بالاعتذار(الذي يحتوي على لهجة سلبية وتعترف بها المنشأة بالذنب)عن خرق البيانات سيؤثر بشكل سلبي على قيمة سهم المنشأة المخترقة(Masuch et al., 2022, p9-11). وأن الإفصاح عن المخاطر السيبرانية يرتبط ارتباطاً إيجابياً بشكل كبير بمخاطر انهيار أسعار أسهم المنشأة بعد سنة من إصدار التقرير السنوي(Song et al., 2020, p6037). ويمكن أن تؤدي انتهاكات البيانات إلى فقدان الدخل/انخفاض سعر سهم المنشآت المدرجة بشكل عام(Legenchuk et al., 2022, p41).

ويكون للإفصاح الضعيف عن المخاطر السيبرانية تأثير محدود على أسعار الأسهم، لكن الإفراط في الإفصاح قد يؤدي إلى نتائج عكسية(Navarro and Sutton, 2021, p281). وتؤثر الهجمات سلبياً على أسعار الأسهم، في حين أن تبرير خرق البيانات ليس له تأثير أو تأثير إيجابي(Masuch et al., 2022, p1;Tsen et al., 2021, p19). ويمكن أن تؤدي الهجمات السيبرانية إلى ظاهرة فريدة-الشهرة السلبية- عندما تكون القيمة السوقية للمنشأة أقل من إجمالي القيمة العادلة لأصولها (Zadorozhnyi et al., 2021, p43). وشهدت المنشآت عوائد سلبية غير طبيعية كبيرة من ١٥٪ إلى ١٨٪ خلال الاثني عشر شهراً التي أعقبت إعلان الخرق، وبالمقارنة زادت مخاطر الأسهم بنسبة ١١٪ في غضون ستة أشهر قبل الإعلان وبعده(Ali et al., 2021, p1).على عكس دراسة(Avery, 2021, p501) أن بعد هذه الفترة تصبح التغييرات التي تطرأ على القيمة السوقية للمنشأة في أسعار الأسهم، غير ذات أهمية إحصائية بحيث لا يمكن ربطها مرة أخرى بحدث الخرق. وأن المنشآت ذات المخاطر السيبرانية الأعلى تكسب

متوسط عوائد أعلى للأسهم، وهو ما لا يمكن تفسيره من خلال نماذج تسعير الأصول(Jiang et al., 2022, p1).

وتشير الدراسات التجريبية الحديثة إلى أنه ليست كل التأثيرات سلبية، على سبيل المثال، فقد أشار (Gay, 2017) إلى أن بعض المؤسسات قد تشهد زيادة في عوائد سوق الأسهم بسبب التغطية الإعلامية الإيجابية بعد حدث الاختراق. ووجدت دراسة(Rosati et al., 2022)أن هذه الإعلانات لها تأثير إيجابي قصير المدى على حجم التداول في يوم الحدث، ولا توجد تأثيرات على اليوم السابق للحدث، ثم تعود بسرعة إلى الحالة الطبيعية بعد يوم الحدث. ولم تؤكد دراسة(Juma'h and Alnsour, 2021, p13) على وجود علاقة جوهرية بين خروقات البيانات ورد فعل سوق الأسهم عند حدوث إختراق سيبراني، وقد يتفاعل المستثمرون في أسواق الأسهم مع إعلانات خرق البيانات بشكل يومي وليس على أساس ربع سنوي. ومع ذلك عندما تتعرض المنشأة لهجمات سابقة ، قد يدرك المستثمرون أن خطر الهجوم السيبراني أعلى بالنسبة لمثل هذه المنشأة ، مما يؤدي إلى علاوة أعلى في أسعار الأسهم للإفصاح عن الاستراتيجية المخففة (Cao et al., 2023, p6081). ولم تجد دراسة(Schuurman, 2020, p24) أي تأثيرات جوهرية على سعر السهم بعد الإعلان عن الخروقات الأمنية في الفترة المدروسة لنوافذ الأحداث المتعددة. وتصبح العوائد غير الطبيعية غير ذات أهمية بالنسبة لخروقات البيانات للمرة الثانية، ويمكن أن يُعزى ذلك إلى أن المستثمرين لم يعودوا متفاجئين، أو أنهم تفاعلوا بالفعل بشكل كافٍ بعد الانتهاك الأول، ويمكن أن تكون المنشآت قد تعلمت بمرور الوقت استخدام الأخبار الإيجابية لتعويض ردود الفعل السلبية في السوق(Peng et al., 2022, p5-6).

وبناءً على ما تقدم، يتضح للباحث أهمية دراسة وتحليل أثر الإفصاح عن المخاطر السيبرانية على القيمة السوقية في المنشآت المدرجة بالبورصة المصرية، نظراً لأنه لا يوجد حتي الآن- في حدود علم الباحث- أيه دراسة عربية أو مصرية، تناولت هذه العلاقة.

٢/٣/٥- إنعكاسات الإفصاح عن إدارة المخاطر السيبرانية على قيمة المنشأة

إن المنشآت التي تفصح وتظهر الوعي بالأمن السيبراني، من خلال تبني سياسات وتدابير الأمن السيبراني، وتنفيذ الإفصاح الفعال عن المخاطر السيبرانية وإدارتها، وبالتالي، فإنهم في وضع أفضل لمنع وقوع أو تقليل تكلفة الحادث السيبراني، ولديها تقييم أعلى من قبل السوق(Berkman et al., 2018, p512, 522). وأن الإفصاح المتعلق بالأمن السيبراني في التقارير السنوية يرتبط إيجابياً بالقيمة السوقية للمنشأة، وأن الإفصاح عن إجراءات الأمان الاستباقية له التأثير الأكبر ;Gordon et al., 2018, p510 (Navarro, 2019, p13). وتوصلت دراسة(Kelton, 2021) إلى أن الإفصاحات حول جهود إدارة المخاطر السيبرانية، توفر حماية للشركات من آثار العدوى، وعندما يحدث خرق في شركة نظيرة في الصناعة، ينظر المستثمرون إلى المنشأة غير المخترقة، والتي تقدم إفصاحات عن الأمن السيبراني بشكل إيجابي أكثر من تلك التي لا تقدم إفصاحات.

ويمكن أن يقدم الإفصاح عن المخاطر السيبرانية أيضاً إشارة إيجابية إلى السوق، من خلال إبلاغ المساهمين بوعي المنشأة والجهود المبذولة لتقليل المخاطر السيبرانية، وفي هذا السياق، قد تميل المنشآت التي تقر وتفصح عن المخاطر السيبرانية، إلى بذل جهود للحد من هذه المخاطر، وتوصلت إلى أن وعي المنشآت بالأمن السيبراني والمخاطر يرتبط ايجابياً بالقيمة السوقية للمنشأة(Cheong et al., 2021,p186-187). وتوصلت دراسة(Gatzert and Schubert, 2022, p743,746) إلى وجود علاقة إيجابية ودالة إحصائياً بين إدارة المخاطر السيبرانية وTobin's Q، حيث تتمتع المنشآت التي لديها إدارة للمخاطر السيبرانية بنسبة ١١٪ أعلى من Tobin's Q مقارنة بالمنشآت التي لا تمتلك إدارة للمخاطر السيبرانية. حيث ينظر السوق بإيجابية إلى إفصاحات المنشآت التي تنقل مستوى أعلى من الوعي بالأمن السيبراني(Barry et al., 2022, p1). وعندما يكون لدى المنشآت مجلس إدارة أكثر كفاءة في مجال تكنولوجيا المعلومات، فإن التوقعات المسبقة للمستثمرين في الأسهم، للإشراف الفائق على تكنولوجيا المعلومات من قبل مجلس الإدارة يتم وضعها في أسعار أسهم تلك المنشآت (Benaroch and Fink, 2021, p2).وأخيراً، توصلت دراسة(Cao et al., 2023, p6084) إلى أن مناقشة استراتيجيات الأمن

السيبراني في تقارير (10-K)(تحديد الهوية والكشف والاستجابة والتعافي)مرتبطة بشكل إيجابي وكبير بالقيمة السوقية للمنشأة (CARs)حول تاريخ إصدار التقرير، وتعد علامة على أن المنشأة تولي مزيداً من الاهتمام لاكتشاف الحوادث السيبرانية، وتجعل المستثمرين ينظرون إلى المنشأة التي تعرضت للهجوم بشكل أفضل.

ويرى الباحث أن تقييم الإدارة للمخاطر السيبرانية يعني وجود إجراءات للتعامل معها في حالة حدوثها، ويجبرها على أن يكون لديها استراتيجيات طارئة.

سادساً: الدراسة التطبيقية واختبارات الفروض.

١/٦- منهجية الدراسة التطبيقية

تناول الباحث من خلال الجانب النظرى للبحث تأصيلاً علمياً للإطار النظري لموضوع البحث، وذلك من خلال ماتم تناوله من طبيعة وتصنيفات المخاطر السيبرانية، والتي تهدد حماية المعلومات المحاسبية في القطاعات المختلفة، وتحليل الآثار المحتملة للمخاطر السيبرانية على النظام المحاسبي، تحليلاً مجملاً لطبيعة ومداخل القياس الكمي للمخاطر السيبرانية، وتحليل متطلبات الإفصاح والتقرير عن المخاطر السيبرانية وحوكمة إدارتها، وقيمة المنشأة من منظور محاسبي(بين المفهوم ومداخل القياس)، و تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وقيمة المنشأة.

وتتحقق قيمة البحث العلمي من خلال ربط الجوانب النظرية بالجوانب العملية بحيث يكتمل موضوع البحث ويحقق أهدافه، وفى ضوء ما سبق واستكمالاً للفائدة المرجوة من البحث يري الباحث ضرورة التأكد من صحة ما تم التوصل إليه من خلال الدراسة النظرية بالإضافة لاختبار فروض البحث وذلك من خلال الاتجاه للواقع العملي واجراء دراسة تطبيقية على عينة من شركات المساهمة المسجلة في البورصة المصرية والتي تمثل قطاعى البنوك والإتصالات وتكنولوجيا المعلومات، **وحتى تحقق الدراسة التطبيقية الهدف منها فلابد من تناول منهجية الدراسة التطبيقية والنماذج الكمية التي تعبر عن فروض البحث، وذلك من خلال تناول النقاط التالية:**

١/١/٦- هدف الدراسة التطبيقية

يتمثل الهدف العام للدراسة التطبيقية في قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشأة، وذلك بالتطبيق على قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات' خلال السنوات المالية ٢٠١٩، ٢٠٢٠،٢٠٢١، **ولذلك يشتق من هذا الهدف أهداف فرعية هي:**

تحليل المحتوي الوصفي للتقارير المالية المنشورة الكترونياً لشركات العينة خلال السنوات المالية ٢٠١٩،٢٠٢٠،٢٠٢١، وذلك لتحليل وتقييم مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية، وذلك بالاعتماد على مؤشر مقترح من الباحث لقياس الإفصاح الإلكتروني عن المخاطر السيبرانية، وقياس درجة التفاوت (التمايز) بين شركات العينة عند الإفصاح الإلكتروني عن المخاطر السيبرانية.

قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشأة وذلك لشركات عينة الدراسة.

٢/١/٦- فروض الدراسة التطبيقية:

في ضوء الإطار النظري للبحث واستنادًا إلى الأهداف التي يسعى الباحث لتحقيقها، يمكن صياغة الفروض التالية:

الفرض الأول: يوجد تفاوت في الإفصاح الإلكتروني عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.

الفرض الثانى: يوجد ارتباط معنوي بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة.

الفرض الثالث: يوجد أثر ذو دلالة إحصائية للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة.

٣/١/٦- مجتمع وعينة الدراسة:

حدد الباحث مجتمع الدراسة التطبيقية في شركات المساهمة المقيدة في البورصة المصرية والعاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية، والتي تقدم خدمات الدفع الإلكتروني، والخدمات الرقمية، وتقديم تكنولوجيا الاتصالات والمعلومات، عبر مواقعها، وبالتالي تعرضها للمخاطر السيبرانية، و بعد قيام هيئة سوق المال بإعادة هيكلة قطاعات البورصة المصرية(*)، **أصبحت القطاعات الأقرب إلى هدف البحث؛ هي قطاع المؤسسات المالية المصرفية (البنوك) والتي بلغ عددها (١٤) بنك، بالإضافة إلى قطاع الاتصالات والاعلام وتكنولوجيا المعلومات والتي بلغ عددها (٦) شركات، ليصبح عدد الشركات الممثلة لمجتمع الدراسة (٢٠) شركة**(البورصة المصرية: https://www.egx.com.eg).

وقام الباحث باختيار شركات المساهمة المسجلة في البورصة المصرية كمجتمع للدراسة واستبعد التطبيق على الشركات غير المدرجة في البورصة وذلك للأسباب التالية:

اختيار الشركات المقيدة في البورصة يضمن وجود وحدات تكنولوجيا المعلومات والتقنيات الحديثة بها واستخداماها التكنولوجيا الرقمية، مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية وخدمات الدفع الإلكتروني، ومن ثم احتمالية تعرضها للمخاطر السيبرانية.

اختيار الشركات المقيدة في البورصة يضمن الوصول لمكاتب المراجعة الكبرى؛ حيث تراجع هذه الشركات بواسطة مكاتب مراجعة ترتبط بمكاتب المراجعة الكبرى (BIG4)، ومن ثم جودة التقارير المالية، مما يتيح الفرصة لإمكانية تشغيل النموذج المقترح لقياس الإفصاح الإلكتروني للمخاطر السيبرانية، من خلال تحليل المحتوى المعلوماتي للتقارير المالية.

وقد قام الباحث باختيار عينة من تلك الشركات وفقاً لمدى استيفاء الشركات لمجموعة من المحددات والضوابط والتي يجب أخذها في الاعتبار عند تعميم نتائج الدراسة (*)**، وهى:**

- ✓ أن تكون أسهم تلك الشركات مقيدة ببورصة الأوراق المالية المصرية ضمن مؤشر البورصة (EGX100)، وتكون خاضعة للتداول داخل المؤشر طوال فترة الدراسة.
- ✓ استبعاد شركات قطاع الخدمات المالية غير المصرفية لما لهما من خصائص تميز طبيعة عملهما، والتي تنعكس على المعلومات الواردة فى التقارير المالية، بالإضافة إلى اختلاف المتطلبات القانونية والتنظيمية التى تخضع لها هذه المؤسسات.
- ✓ أن تكون الشركة قد مضى على قيدها في البورصة أكثر من ثلاثة سنوات وهى مدة الدراسة، وألا تكون قد تعرضت للشطب أو الاندماج أو التوقف خلال فترة الدراسة.
- ✓ أن تتوافر التقارير المالية وتقرير مجلس الإدارة وتقارير الاستدامة ونشرات الإعمال للشركة بانتظام، والافصاح عنها بالعملة المصرية من خلال موقع الشركة الإلكتروني على شبكة الأنترنت، وأن تتوافر فيها بيانات كافية لحساب متغيرات الدراسة.

(*) **يراجع جداول الشركات المدرجة في السوق الرئيسى للسنوات (٢٠١٩ – ٢٠٢١) على موقع البورصة المصرية على شبكة الإنترنت (تاريخ زيارة الموقع ٢٠٢٣/٤/١) من خلال الرابط التالى:**
https://www.egx.com.eg/ar/Disclosure_Reports.aspx

(*) **أن قابلية نتائج الدراسة التطبيقية للتعميم مشروطة بضوابط ومحددات اختيار عينة الدراسة**، حيث أن الاعتماد على ضوابط أخرى ستؤدى إلى عينة مختلفة من الشركات يمكن في بعض الأحوال أن يؤدي إلى نتائج مختلفة.

وقد أسفر تطبيق المعايير السابقة عن اختيار عدد (٨) بنوك و(٦) شركات تكون (٤٢) مشاهدة لتمثل عينة الدراسة، ويوضح الجدول التالي أسماء البنوك والشركات الممثلة في عينة الدراسة، وذلك كما يلى:

الجدول رقم (٦)

أسماء البنوك والشركات الممثلة في عينة الدراسة

م	القطاع	اسم الشركة	كود رويترز	كود الترقيم الدولى	تاريخ القيد في البورصة
	قطاع البنوك (٨ بنوك)	البنك التجاري الدولي- مصر	COMI.CA	EGS60121C018	١٩٩٥/٠٢/٠٢
		بنك الشركة المصرفية العربية الدولية	SAIB.CA	EGS60142C014	١٩٨٠/١١/٢٩
		بنك أبو ظبي التجاري	ADIB.CA	EGS60111C019	١٩٩٦/٠٦/١٩
		بنك التعمير والإسكان	HDBK.CA	EGS60301C016	١٩٨٣/٠٩/١٣
		بنك الكويت الوطنى مصر	NBKE.CA	EGS60171C013	١٩٩٤/٠٩/١
		بنك قناة السويس	CANA.CA	EGS60231C015	١٩٨٢/٠٩/١٥
		بنك قطر الوطنى الأهلى	QNBA.CA	EGS60081C014	١٩٩٦/٠٧/٠٣
		بنك كريدي أجريكول مصر	CIEB.CA	EGS60041C018	١٩٩٦/٠٧/٠٣
	قطاع الاتصالات وتكنولوجيا المعلومات (٦ شركات)	المصرية للأقمار الصناعية (نايل سات)	EGSA.CA	EGS48022C015	١٩٩٨/١٢/٠٩
		المصرية للاتصالات	ETEL.CA	EGS48031C016	١٩٩٩/١٢/٢٩
		فوري لتكنولوجيا البنوك والمدفوعات الالكترونية	FWRY.CA	EGS745L1C014	٢٠١٩/٠٧/٢٨
		المصريه لمدينة الانتاج الاعلامى	MPRC.CA	EGS78021C010	١٩٩٩/٠٩/٢٦
		اوراسكوم للاستثمار القابضه	OIH.CA	EGS693V1C014	٢٠١٢/٠١/٠٢
		راية لخدمات مراكز الاتصالات	RACC.CA	EGS74191C015	٢٠١٥/٠٢/١١
	الإجمـالي		١٤ شركة * ٣ سنوات = ٤٢ مشاهدة		

المصدر: الباحث، مسترشداً بموقع البورصة المصرية: https://www.egx.com.eg.

٤/١/٦- مصادر الحصول على البيانات:

اعتمدت الدراسة التطبيقية **على أسلوب تحليل المحتوي الوصفى** في قياس مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية، من خلال تفريغ النموذج المقترح من الباحث لهذا الغرض، **بالإضافة إلى تحليل المحتوى للتقارير المالية والسنوية للشركة**، والمعلومات المتوفرة على الموقع الإلكتروني للشركة، والمعلومات المتوفرة على موقع البورصة المصرية https://egx.com.eg، ومواقع التحليل الإحصائي ذات الصلة؛ مثل موقع مباشر مصر www.Mubasher.info، وموقع شركة https: sa.investing.com، وذلك لاستيفاء البيانات الكمية لباقي متغيرات البحث.

٥/١/٦- طرق قياس متغيرات الدراسة:

يمكن للباحث، توضيح طريقة قياس متغيرات الدراسة، ومبررات اختيار المتغيرات الرقابية كما يلى:

١- المتغير المستقل: الإفصاح الإلكتروني عن المخاطر السيبرانية (CRD):

على الرغم من عدم وجود تقرير خاص أو شكل معين للإفصاح الإلكتروني عن المخاطر السيبرانية في بيئة الأعمال المصرية في الوقت الحالي، إلا أن بعض الشركات تنشر معلومات عن المخاطر السيبرانية وفعالية ادارتها ضمن الإيضاحات المتممة للقوائم المالية، وكذلك ضمن تقرير مدى الالتزام بقواعد الحوكمة، وكذلك تقرير مجلس الادارة وغيرها من التقارير ذات الصلة سواء بشكلها التقليدي أو إلكترونياً من خلال موقع الشركة على الإنترنت، وفى ضوء ذلك قام الباحث بإتباع نفس نهج العديد من الدراسات السابقة؛ بتكوين مؤشر لقياس مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية بالشركات المقيدة فى البورصة يتكون من (٥٣) بند يعتمد على مايلى:

- **إصدارات الهيئات المهنية**، مثل: (المعهد الأمريكي للمحاسبين القانونيين(AICPA, 2017). والدليل الارشادي لمعهد المحاسبين القانونين الكندي(CPA.CANDA, 2017) للإفصاح عن المخاطر السيبرانية. و تقرير مجلس التقارير المالية(FRC) الصادر في أغسطس ٢٠٢٢. والدليل الإرشادي لـ(SEC, 2011; 2018). وفي ضوء تكامل إطار COBIT.5، ومعايير الآيزو ISO 27001،

وسلسلةNIST SP 800 . ومؤشر الإفصاح عن المخاطر السيبرانية لبورصة تورنتو (TSX) الكندية.

- **الاستراتيجية المصرية للأمن السيبراني(٢٠١٧-٢٠٢١)**، وذلك لمراعاة ظروف البيئة المصرية في المؤشر.
- **الموشرات الأخرى**، التى إستخدمتها الدراسات السابقة في قياس مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية (يعقوب وآخرون، ٢٠٢٢؛ Berkman et al., 2018; Bodin et al., 2018; Li et al.,2018; Skinner, 2019; Gao et al., 2020; Héroux and Forting, 2020; Heidenborg and Lappalainen, 2021; Eijkelenboom and Nieuwesteeg, 2021; Radu and Smaili, 2022; Sebastian, 2022 ; Ramírez et al., 2022;Cao et al., 2023, p6084))

ويتكون المؤشر المقترح من **المحاور الخمس** التالية، وهي:(قنوات الاتصال الإلكترونية للشركة (٨ بنود)، و المخاطر السيبرانية الفعلية والمحتملة (١١ بند)، و الآثار المحتملة للمخاطر السيبرانية (٦ بنود)، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (١٣ بند)، وأخيراً تخفيف المخاطر السيبرانية(١٥ بند)).

ويستند المؤشر إلى المدخل الثنائي غير المرجح الذي يعامل جميع العناصر بأهمية متساوية رغم تفاوت أهميتها ويعطي نتائج دقيقة عن غيره من المقاييس الأخرى فى ظل عدم وجود ألية تسمح بالقياس الكمي للفروق بين تلك العناصر وذلك كما يلى:

- ✓ إعطاء متغير وهمى للبنود التي يحتويها المؤشر بحيث يتم إعطاء القيمة (١) إذا كانت الشركة تفصح عن البند أو ما يدل على وجوده وإعطاء القيمة (٠) إذا كانت الشركة لا تفصح عن البند (البند غير موجود).
- ✓ تجميع الدرجات لكل شركة ونسبتها إلى الحد الأقصى للبنود الواجب الإفصاح عنها وهى ٥٣ بند، ومن ثم يمكن حساب مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية لكل شركة وذلك من خلال المعادلة التالية:

مستوي الإفصاح عن المخاطر السيبرانية وفقاً المؤشر المقترح = (إجمالي بنود الإفصاح الفعلي من قبل الشركة/ إجمالي درجات بنود الإفصاح بالمؤشر(٥٣ بند))×١٠٠

٢- المتغير التابع: قيمة المنشاة (FV)

تم قياس هذا المتغير باستخدام نموذج(*Tobin's Q*) وهو مقياس للقيمة السوقية للمنشأة ويحسب قيمة المنشأة من خلال المعادلة الأتية:(القليطي، ٢٠١٩، ص ٤١؛ عازر، ٢٠٢٢، ص٥٦؛ Hapsoro and Bahantwelu, 2020, p. 61; Kamiya et al. 2021, p729; Tosun et al. 2021, p2; ; Gatzert and Schubert, 2022, p733; Florackis et al., 2022, p403; Bamiatzi et al., 2023, p15):

$$\textbf{Tobin's Q} = \frac{\text{القيمة السوقية لحقوق الملكية + القيمة الدفترية لإجمالى الإلتزامات}}{\text{القيمة الدفترية لإجمالى الأصول}}$$

٣- المتغيرات الرقابية (CONTROL VARIABLE): تشمل المتغيرات الرقابية بعض العوامل المؤثرة على المتغيرات التابعة (قد تكون ذات تأثير محتمل على قيمة المنشأة)، ولكنها لا تدخل في نطاق الدراسة محل البحث، وتم إضافتها من أجل ضبط العلاقة بين المتغير المستقل والمتغير التابع، ومن أهم هذه المتغيرات:(حجم الشركة وربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات)، ويمكن تناول طرق قياس هذه المتغيرات ومبررات ادخالها في العلاقة بين المتغير المستقل والمتغير التابع، كما يلى:

- **حجم الشركة (FSIZE):** وتعبر عن القدرات والامكانيات المادية والبشرية والتكنولوجية للشركة والتى تؤثر على قيمة الشركة في السوق، بالإضافة إلى أن الشركات الكبيرة الحجم تستخدم نظم معلومات متطورة، ولديها هيكل رقابة داخلية قوي، وتحرص على الإفصاح عن المخاطر السيبرانية، ومن ثم تحسين قيمتها في السوق أمام المساهمين)؛ حيث تواجه الشركات الكبيرة عدداً

متزايداً من المخاطر بالإضافة إلى تعقيدها، ولديهم أيضاً موارد مالية كبيرة، مما يجعلهم أكثر احتمالاً لتنفيذ نظام إدارة مخاطر المؤسسات، ويكشف البحث التجريبي في مجال المخاطر الإلكترونية أن حجم الشركة يلعب دوراً مهماً فيما يتعلق بحدوث حوادث المخاطر السيبرانية، والشركات الكبيرة التي لديها عدد أكبر من الموظفين تعاني من مخاطر سيبرانية بشكل متكرر(Kamiya et al., 2021, p727). **ويقاس حجم الشركة باللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام**. (; McShane and Nguyen, 2020, p580; Kamiya et al., 2021, p724; Gatzert and Schubert, 2022, p731).

- **ربحية الشركة (ROA)**: ويعبر عنه بمعدل العائد على الأصول والذى يدل على جودة الأداء المالى للشركة ويوثر على سمعة وأداء الشركة في السوق ، **ويحسب الأداء المالى من خلال صافي ربح العام قبل الضرائب مقسوما على إجمالي الأصول**(McShane and Nguyen, 2020, p580; Kamiya et al., 2021, p724).
- **درجة الرفع المالى (LEV)**: تشير الرافعة المالية إلى استخدام الموارد المالية مثل (الديون والأموال المقترضة) لزيادة العائد على الأصول؛ حيث تحتاج الشركة إلى إدارة أصولها بكفاءة لتحقيق أهدافها ومواجهة المنافسة في الأسواق المحلية والدولية، ومن ثم فقد أصبحت الرافعة المالية عامل مهم في تحديد القيمة السوقية للشركة، ووجدت دراسة كل من(Kamiya et al., 2021, p724; Gatzert and Schubert, 2022, p739) علاقة إيجابية جوهرية بين الرافعة المالية ووقوع الإنتهاكات السيبرانية، مما قد يشير إلى عدم وجود إدارة للمخاطر السيبرانية، **ويتم قياس درجة الرفع المالي للشركة من خلال قسمة إجمالي الالتزامات على إجمالي الأصول**. (Ali et al., 2022, p37, Vincent and Trussel, 2019, p495).
- **جودة حوكمة الشركات (CGQ):** ويعتبر من المتغيرات التي تؤثر على قيمة المنشأة، حيث أن الشركات التى تلتزم بتطبيق آليات الحوكمة ينتظم بها سير العمل، وتحافظ علي إستقلالية أعضاء لجنة المراجعة، كما أنها تضمن توافر الخبرات المالية والمحاسبية داخل لجان المراجعة، بما يساهم في سلامة وصحة القرارات المالية؛ وبالتالي جودة القوائم المالية وتحسين مستوى الإفصاح بشكل عام، **واستخدم الباحث مؤشر تجميعي لقياس جودة آليات الحوكمة داخل الشركة، حيث يأخذ القيمة من (صفر) إلى(١٠) حسب مدي توافر مؤشرات جودة الحوكمة**، والتى تتمثل فى استقلال أكثر من نصف أعضاء المجلس، وعدم الجمع بين منصبي رئيس مجلس الإدارة والعضو المنتدب، وعدد أعضاء لجنة المراجعة لا يقل عن ثلاثة أعضاء، واستقلال أعضاء اللجنة، وتوافر الخبرات المالية والمحاسبية في أعضاء اللجنة، وعدد مرات اجتماع لجنة المراجعة لا يقل عن (٤) مرات سنوياً، وجود دليل عمل للجنة المراجعة، وجود لجنة للحوكمة، وجود لجنة لإدارة المخاطر، ارتباط الشركة بأحد مكاتب المراجعة الكبرى (الدليل المصري لحوكمة الشركات- الإصدار الثالث، ٢٠١٦ ؛ Gatzert and Schubert, 2022, p731).

ويمكن للباحث توضيح طريقة قياس متغيرات الدراسة من خلال الجدول التالي:

الجدول رقم (٧)

التعريف الإجرائي بمتغيرات الدراسة

المتغيرات	الرمز	طريقة القياس	نوع المتغير	مصدر الحصول على البيانات
أولا: المتغير التابع :(قيمة الشركة FV)				
قيمة المنشأة	FV	يتم قياس هذا المتغير باستخدام نموذج (Tobin's Q) وهو مقياس للقيمة السوقية للمنشأة ويحسب قيمة المنشأة من خلال المعادلة الآتية Tobin's Q= (القيمة السوقية لحقوق الملكية +القيمة الدفترية لإجمالى الإلتزمات)/(القيمة الدفترية لإجمالى الأصول)	تابع	التقارير المالية للشركات
ثانيا: المتغير المستقل :(الإفصاح الإلكتروني عن المخاطر السيبرانية)				
الإفصاح الإلكتروني عن المخاطر السيبرانية	CRD	قام الباحث بإتباع نفس نهج العديد من الدراسات السابقة بتكوين مؤشر لقياس مستوى الإفصاح الإلكتروني عن المخاطر السيبرانية بالشركات المقيدة فى البورصة يتكون من (53) بند ويتكون المؤشر المقترح من المحاور الخمس التالية، وهي:(قنوات الاتصال الإلكترونية للشركة (٨ بنود)، والمخاطر السيبرانية الفعلية والمحتملة (١١ بند)، و الآثار المحتملة للمخاطر السيبرانية (٦ بنود)، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (١٣ بند)، وأخيراً تخفيف المخاطر السيبرانية (١٥ بند)).	مستقل	التقارير المالية وغير المالية للشركة والمواقع الإلكترونية للشركات
ثالثاً: المتغيرات الحاكمة : (المتغيرات الرقابية)				
حجم الشركة	FSIZE	يقاس باللوغاريتم الطبيعى لإجمالى الأصول.	متغيرات (رقابية)	التقارير السنوية والإيضاحات المتممة للقوائم المالية
ربحية الشركة	ROA	يقاس من خلال صافي ربح العام قبل الضرائب مقسوما على إجمالي الأصول		
درجة الرفع المالي	LEV	يقاس بنسبة إجمالى الالتزامات على إجمالى الأصول .		
جودة خصائص الحوكمة	CGQ	استخدم الباحث مؤشر تجميعي لقياس جودة آليات الحوكمة داخل الشركة، حيث يأخذ القيمة من (صفر) إلى(١٠) حسب مدي توافر مؤشرات جودة الحوكمة والتى تتمثل فى استقلال أكثر من نصف أعضاء المجلس، وعدم الجمع بين منصبي رئيس مجلس الإدارة والعضو المنتدب، وعدد أعضاء لجنة المراجعة لا يقل عن ثلاثة أعضاء، واستقلال أعضاء اللجنة، وتوافر الخبرات المالية والمحاسبية في أعضاء اللجنة، وعدد مرات اجتماع لجنة المراجعة لا يقل عن (٤) مرات سنويًا، ووجود دليل عمل للجنة المراجعة، ووجود لجنة للحوكمة، ووجود لجنة لإدارة المخاطر، ارتباط الشركة بأحد مكاتب المراجعة الكبري		

المصدر: الباحث، إعتماداً على الدراسات ذات الصلة.

٦/١/٦- نموذج الدراسة التطبيقية: أخذاً فى الإعتبار أن الفرض الأول لا يحتاج إلى بناء نموذج كمى؛ حيث أنه يتم إختباره من خلال دراسة مدى وجود تباين بين شركات العينة حول الإفصاح الإلكترونى عن المخاطر السيبرانية، ينشأ نموذج أساسي للبحث يهدف إلى قياس أثر الإفصاح الإلكترونى عن المخاطر السيبرانية على قيمة المنشاة في ضوء العوامل الرقابية، ويغطى هذا النموذج الفرض الثالث للدراسة، ويمكن التعبير عن النموذج بالمعادلة الكمية التالية:

$$FV = \beta_0 - \beta_1 (CRD) + \beta_2 (FSIZE) + \beta_3 (ROA) + \beta_4(LEV) + \beta_5(CGQ) + \varepsilon_{it}$$

حيث (**FV**): المتغير التابع وهو قيمة المنشاة ، **CRD**: المتغير المستقل وهو الإفصاح الإلكترونى عن المخاطر السيبرانية، (**FSIZE**) هو حجم الشركة، (**ROA**) ربحية الشركة، (**LEV**) درجة الرفع المالى للشركة،(**CGQ**) جودة حوكمة الشركات، والباحث إفترض مبدئيا وجود علاقة إيجابية بين جميع المتغيرات المستقلة والمتغير التابع.

٦/٢- تحليل نتائج الدراسة واختبار الفروض: قام الباحث بتطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية [Statistical Package for Social Science (SPSS)] (**الإصدار (٢٥) فى تحليل البيانات إحصائيا**) وقد تطلبت طبيعة البيانات تحديد الأساليب الإحصائية اللازمة والملائمة، والتي تتمثل فيما يلي: (سليمان، ٢٠٠٧، Abu-Bader,2021)

- **تحديد مدى صلاحية البيانات للتحليل الإحصائى** من خلال إختبار مدى إتباع البيانات للتوزيع الطبيعى وذلك لتحديد نوع الإختبارات المستخدمة بعد ذلك، وقياس القدرة التفسيرية لنماذج الدراسة، بالإضافة إلى أختبار التداخل أو الازدواج الخطي والإرتباط الذاتي لنماذج الدراسة.
- **توصيف المتغيرات الكمية والوصفية للدراسة من خلال أساليب الإحصاء الوصفي** وأهمها الوسط الحسابي، الانحراف المعياري، وأعلى قيمة وأقل قيمة.
- **تحديد مدى الاتفاق أو الإختلاف بين قطاعات عينة الدراسة حول الإفصاح الإلكترونى عن المخاطر السيبرانية** وذلك من خلال إختبارات الفروق وأهمها اختبار (Mann-Whitney Test)، وذلك لإختبار الفرض الأول.
- **إختبار فرضى الدراسة الثانى والثالث من خلال أساليب الإحصاء الاستدلالي؛** وأهمها تحليل الارتباط (Correlation analysis)، وتحليل الانحدار (Simple Regression Model) مع التركيز على معامل التحديد (R Square)، وذلك كما يلي:

١/٢/٦- إختبار صلاحية البيانات للتحليل الإحصائي: ويتم ذلك من خلال القيام بما يلي:

١- اختبار مدى إتباع البيانات للتوزيع الطبيعي (Normal Distribution Test): للتحقق من مدى اقتراب البيانات من توزيعها الطبيعي تم استخدام اختبار **(Kolmogorov – Smirnov)** واختبار **(Shapiro–Wilk)** للتأكد من أن نمط التوزيع الذي تسلكه بيانات الدراسة هو توزيع طبيعي وذلك بالنسبة لمتغيرات الدراسة، وذلك لتحديد نوع الاختبارات التي سيستخدمها الباحث في التحليل الإحصائي للبيانات مابين اختبارات الإحصاء المعلمى واختبارات الإحصاء اللامعلمى، والجدول التالي يوضح قيم الاختبارات ومستوى المعنوية لكل متغير أمام كل اختبار:

الجدول رقم (٨)

التوزيع الطبيعي لمتغيرات الدراسة

Variables		Kolmogorov-Smirnov Statistic		Shapiro-Wilk Statistic	
		Value	Sig.	Value	Sig.
الإفصاح الإلكتروني عن المخاطر السيبرانية	CRD	٠,٢٦٥	٠,٠٠٠	٠,٨٢٧	٠,٠٠٠
قيمة المنشأة	FV	٠,٤٢٣	٠,٠٠٠	٠,٤٢٩	٠,٠٠٠
حجم الشركة	FSIZE	٠,١٦٨	٠,٠٠٤	٠,٩٤٨	٠,٠٥٥
ربحية الشركة	ROA	٠,١٨٠	٠,٠٠٢	٠,٨٧٧	٠,٠٠٠
درجة الرفع المالى	LEV	٠,٢٩٥	٠,٠٠٠	٠,٧٠٣	٠,٠٠٠
جودة حوكمة الشركات	CGQ	٠,٢٠٣	٠,٠٠٠	٠,٨٨٨	٠,٠٠١

المصدر: نتائج التحليل الاحصائي.

ويتضح من الجدول السابق أن قيمة مستوى المعنوية (.Sig) لاختبار (Kolmogorov-Smirnov) واختبار (Shapiro-Wilk) أقل من (٠,٠٥) لجميع المتغيرات، وبناءً على ذلك فإن البيانات الخاصة بمتغيرات الدراسة لا تتبع التوزيع الطبيعي، وبناءا على النتيجة السابقة فإن البيانات الخاصة بمتغيرات الدراسة لاتتبع التوزيع الطبيعي، ولخفض أثر مشكلة عدم خطية البيانات قام الباحث بإستخدام التحويلات الإحصائية (**Tansformation**) من خلال أخذ اللوغاريتم الطبيعى لبعض المتغيرات (**Log**) وذلك لجعل التباين أكثر إستقرارا وتقريب البيانات من العلاقة الخطية (الزغبى ، الطلاحفة، ٢٠١٢)، **وفى ضوء ماسبق يلتزم الباحث** عند إختبار الفروق المرتبطة بالمتغيرات التى لاتتبع بياناتها التوزيع الطبيعى إستخدام الإختبارات اللامعلمية.

٢- اختبار التداخل أو الازدواج الخطي (Collinearity Test): يتم التحقق من مشكلة التداخل أو الازدواج الخطي بين المتغيرات المستقلة من خلال اختبار (**Multicollinearity Test**) والذي من خلاله يتم حساب معامل تضخم التباين (**Variance Inflation Factor (VIF)**) لكل متغير من المتغيرات المستقلة التى تؤثر في المتغير التابع، وذلك لنماذج الدراسة كما يلى:

الجدول رقم (٩)
نتائج اختبار (M. C. Test) لنماذج الدراسة

المتغيرات المستقلة فى نموذج الدراسة (مستقلة ورقابية)			نتائج إختبار التداخل الخطى Collinearity Test	
			المتغير التابع: قيمة المنشأة (FV)	
المتغير المستقل	الإفصاح الإلكترونى عن المخاطر السيبرانية	CRD	Tolerance	VIF
متغيرات رقابية	حجم الشركة	FSIZE	٠,٤١٤	٢,٤١٦
	ربحية الشركة	ROA	٠,٦٦٨	١,٤٩٦
	درجة الرفع المالى	LEV	٠,٤٧٥	٢,١٠٦
	جودة حوكمة الشركات	CGQ	٠,٤٤٢	٢,٢٦٢

المصدر: نتائج التحليل الاحصائي.

يتضح للباحث من الجدول السابق أن قيم (VIF) لجميع المتغيرات المستقلة ومتغيرات الرقابة في نموذج الدراسة أقل من (١٠) ، وهذا يعني أن المتغيرات المستقلة في كل نموذج لا تعاني من مشكلة التداخل أو الازدواج الخطي فالارتباط بينها ليس له دلالة إحصائية ومنخفض جدًا، الأمر الذي يدل على قوة النموذج المستخدم في تفسير وتحديد تأثيرات المتغيرات المستقلة على المتغيرات التابعة.

٣- اختبار الارتباط الذاتي (Autocorrelation Test): للتحقق من خلو متغيرات الدراسة في كل النماذج من مشكلة الارتباط الذاتي تم استخدام اختبار(**Durbin Watson Test**)، وهو ما يتضح من الجدول التالي:

الجدول رقم (١٠)
نتائج اختبار الارتباط الذاتي (Durbin Watson Test)

	نتائج اختبار الارتباط الذاتي Durbin Watson Test
	المتغير التابع: قيمة المنشأة (FV)
قيمة(D-W)	١,٦٩٠

المصدر: نتائج التحليل الاحصائي.

يتضح للباحث من الجدول السابق أن قيم (D-W) المحسوبة تقترب من المدى المثالي وهو الذي يقع بين (١,٥،٢,٥)، وفقا لجدول (Durbin Watson Test) عند مستوى معنوية (٠,٠٥) مع أخذ في الاعتبار حجم المشاهدات وعدد المتغيرات الداخلة في النموذج، مما يدل على عدم وجود مشكلة للارتباط الذاتي بين المتغيرات المستقلة في نماذج الدراسة تؤثر على صحة النتائج، **وفى ضوء ما سبق يتضح للباحث** أن المتغيرات المستقلة لا تعاني من مشكلة التداخل أو الازدواج الخطي وعدم وجود مشكلة للارتباط الذاتي فيما بينها، وبالتالى قوة نماذج الدراسة وزيادة قدرتها التفسيرية، ومن ثم صلاحية البيانات للتحليل الإحصائي.

٢/٢/٦- التحليل الوصفي لمتغيرات الدراسة: يظهر الجدول التالى نتائج توصيف متغيرات الدراسة وذلك على مدار سنوات الدراسة وعلى مستوى كل المشاهدات (**panel data**)، وذلك كما يلى :

الجدول رقم (١١)
الإحصاء الوصفي لمتغيرات الدراسة

النوع	متغيرات الدراسة	الرمز	السنة		المتوسط الحسابي	الانحراف المعياري	أقصى قيمة	أقل قيمة	التباين
المتغير المستقل	الإفصاح الإلكترونى عن المخاطر السيبرانية	CRD	٢٠١٩	عدد	٢٢,٢٨٦	٩,١٦٩	٤٥	١٢	٨٤,٠٦٦
				نسبة	٠,٤٢	٠,١٧٣	٠,٨٤٩	٠,٢٢٦	٠,٠٣
			٢٠٢٠	عدد	٢٤,٩٢٩	١١,٢٢١	٥٠	١٣	١٢٥,٩١٨
				نسبة	٠,٤٧	٠,٢١٢	٠,٩٤٣	٠,٢٤٥	٠,٠٤٥
			٢٠٢١	عدد	٢٥,٨٥٧	١٢,٠٠٥	٤٩	١٤	١٤٤,١٣٢
				نسبة	٠,٤٨٨	٠,٢٢٧	٠,٩٢٥	٠,٢٦٤	٠,٠٥١
			٢٠١٩-٢٠٢١	عدد	٢٤,٣٥٧	١٠,٧٠٦	٥٠	١٢	١١٤,٦٢٥
				نسبة	٠,٤٦	٠,٢٠٢	٠,٩٤٣	٠,٢٢٦	٠,٠٤١
المتغير التابع	قيمة المنشأة	FV	٢٠١٩		٠,٩٦٧	٠,٨٤٣	٣,٧	٠,٢٣٤	٠,٧١
			٢٠٢٠		١,٤٥٧	٢,٤	٩,٧٣٣	٠,٢٤١	٥,٧٦
			٢٠٢١		١,٠٨٦	١,٢٥٣	٥,٣٠٣	٠,٢٥٢	١,٥٧
			٢٠١٩-٢٠٢١		١,١٧	١,٦١١	٩,٧٣٣	٠,٢٣٤	٢,٥٩٤
المتغيرات الرقابية	حجم الشركة	FISIZE	٢٠١٩		١٩,٧٦٤	٢,٦٩٦	٢٥,٠١٧	١٥,٣١٣	٧,٢٦٩
			٢٠٢٠		١٩,٧٩٢	٢,٦٧١	٢٥,١٥٩	١٥,٢٨٥	٧,١٣٤
			٢٠٢١		١٩,٩٦٥	٢,٦٦٢	٢٥,٢٣١	١٥,٣٢٧	٧,٠٨٤
			٢٠١٩-٢٠٢١		١٩,٨٤١	٢,٦١٢	٢٥,٢٣١	١٥,٢٨٥	٦,٨٢١
	ربحية الشركة	ROA	٢٠١٩		٠,٠٤٥	٠,٠٥٣	٠,١٨٦	-٠,٠٤٦	٠,٠٠٣
			٢٠٢٠		٠,٠٣٣	٠,٠٣٢	٠,١١٤	-٠,٠١٨	٠,٠٠١
			٢٠٢١		٠,٠٤٣	٠,٠٣٩	٠,١٤٧	٠,٠٠٤	٠,٠٠٢
			٢٠١٩-٢٠٢١		٠,٠٤	٠,٠٤٢	٠,١٨٦	-٠,٠٤٦	٠,٠٠٢
	درجة الرفع المالى	LEV	٢٠١٩		١,٢٢٣	٠,٥٣٣	٢,٥١٣	٠,٨٥٧	٠,٢٨٥
			٢٠٢٠		١,٣٦١	٠,٧٩٢	٣,١٧١	٠,٨٥٤	٠,٦٢٧
			٢٠٢١		١,٣٧	٠,٧٤٦	٢,٩٩١	٠,٨٥٦	٠,٥٥٧
			٢٠١٩-٢٠٢١		١,٣١٨	٠,٦٨٦	٣,١٧١	٠,٨٥٤	٠,٤٧
	جودة حوكمة الشركات	CGQ	٢٠١٩		٧,٤٢٩	٠,٨٥٢	٩	٦	٠,٧٢٥
			٢٠٢٠		٨,١٤٣	٠,٧٧	٩	٧	٠,٥٩٣
			٢٠٢١		٨,٥٧١	٠,٨٥٢	١٠	٧	٠,٧٢٥
			٢٠١٩-٢٠٢١		٨,٠٤٨	٠,٩٣٦	١٠	٦	٠,٨٧٦

المصدر: نتائج التحليل الاحصائي.

ويلاحظ من الجدول السابق، أن شركات العينة تفصح عن المخاطر السيبرانية بمتوسط عام بلغ (٢٤,٣٥) بند من إجمالى (٥٣) بند الممثلين للمؤشر المقترح من الباحث بنسبة إفصاح بلغت (٤٦٪) ، ويلاحظ أن هناك تحسن ملحوظ في مستوى الإفصاح الإلكترونى للمخاطر السيبرانية لعينة الدراسة خلال سنوات الدراسة (٢٠١٩: ٢٠٢١)، حيث بلغ متوسط الإفصاح الإلكترونى للمخاطر السيبرانية (٤٢٪)، (٤٧٪)، (٤٨,٨٪)لسنوات الدراسة على الترتيب، ويوضح الإحصاء الوصفى لمتغير الافصاح الإلكترونى للمخاطر السيبرانية، أن الحد الأقصى للإفصاح بلغ (٩٤,٣٪) وتحقق ذلك عام ٢٠٢٠، كما أفصحت شركات العينة بأقل قيمة للإفصاح عند (٢٢,٦٪) وذلك في عام ٢٠١٩.

و**تتفق** هذه النتائج مع دراسة(Héroux and Fortin, 2020)، والتي توصلت أن مستويات الإفصاح عن المخاطر السيبرانية منخفض. على **عكس** دراسة(Eijkelenboom and Nieuwesteeg, 2021)، والتي وتوصلت إلى أنه على الرغم من عدم وجود التزام قانوني للإفصاح عن الأمن السيبراني، فإن ٨٧ ٪ من الشركات تفصح عن ممارسات الأمن السيبراني أو كلمات مشابهة في تقريرها السنوية.

ويقدم الباحث بعض الملاحظات التي يجب أخذها بعين الاعتبار عند توصيف الإفصاح الإلكترونى للمخاطر السيبرانية، والتي لاحظها الباحث عند إستيفاء بنود المؤشر المقترح لقياس مستوى الإفصاح الإلكترونى عن المخاطر السيبرانية لشركات العينة وهى:

- ✓ قيام بعض الشركات مثلا بوضع أيقونة للأمن السيبرانى على الموقع الرسمى للشركة وتركها فارغة دون بيانات وهذا لتضليل مستخدمى الموقع بإهتمام الشركة بالأمن السيرانى وإدارة المخاطر المرتبطة به على غير الحقيقة.
- ✓ تكرار العبارات المتعلقة بالإفصاح عن المخاطر السيبرانية في الإيضاحات المتممة للقوائم المالية على مدار سنوات الدراسة دون إجراء أى تعديلات عليها.
- ✓ عدم وجود بيانات كمية عن الجوانب الهامة للمخاطر السيبرانية، إما في شكل جداول أو أشكال بيانية (الإكتفاء بالإفصاح الوصفى فقط).
- ✓ عدم توافر الضمانات والتأكيدات المستقلة حول معلومات المخاطر السيبرانية المفصح عنها.

وبالنسبة لقيمة الشركة أشارت النتائج إلى وجود تحسن في قيمة (TOBIN Q) كمقياس لقيمة الشركات في السوق حيث بلغت (٠,٩٦٧) في عام ٢٠١٩ وارتفع إلى أن وصل في عام ٢٠٢٠ إلى (١,٤٥٧)، ولكنه انخفض عام ٢٠٢١ وبلغ (١,٠٨٦) ويعزى الباحث هذا الانخفاض إلى احتمالية تأثر أسعار الأسهم نتيجة الأحداث العالمية الناتجة عن الأزمة الروسية الأوكرانية، وما أحدثته من أثار سلبية على أسعار الأسهم وأسواق المال، وعلى المستوى العام لفترة الدراسة بلغت متوسط قيمة (TOBIN Q) لشركات العينة (١,٧) وهى تزيد عن الواحد الصحيح لتدل على إرتفاع القيمة السوقية لشركات العينة في السوق.

وبالنسبة للمتغيرات الرقابية توضح نتائج الجدول السابق أن متوسط اللوغاريتم الطبيعي لإجمالي أصول شركات العينة والدال على حجم الشركة قيمة(١٩,٨٤)، وتؤكد النتائج على ارتفاع حجم الشركات من عام ٢٠١٩ حتى عام ٢٠٢١، حيث بلغ على الترتيب متوسط الأصول (١٩,٧٦)، (١٩,٧٩)، (١٩,٩٦)، **وبالنسبة للأداء المالي للشركات والذى يعبر عنه بربحية الشركة بدلالة معدل العائد على الأصول، توضح النتائج أن ربحية شركات العينة** جاء بمتوسط عائد بلغ (٤٪)، وإن هناك تذبذب في ربحية شركات العينة من عام ٢٠١٩ حتى عام ٢٠٢١ والذى بلغت نسبة الربحية لهذه السنوات على الترتيب (٠,٠٤٥)، (٠,٠٣٣)، (٠,٠٤٣) ، كما حققت شركات العينة أعلى نسبة ربحية وهى (١٨,٦٪) في عام ٢٠١٩ ، والذى شهد أيضا أقل نسبة ربحية لشركات العينة بقيمة (-٠,٠٤٦٪)، **كما بلغت الرافعة المالية، والتي توضح مدي اعتماد الشركة على الديون في تمويل أصولها، فتشير النتائج إلى أن متوسط معدل الرافعة المالية بلغ (١,٣١٨)**، وهو ما يعكس إمكانية قدرة عينة الدراسة في الحصول على التمويل اللازم، وهذه النسبة تدل على مديونية الشركة كأحد العوامل التي تؤثر على قيمة الشركة، ويلاحظ من النتائج زيادة هذه النسبة من سنة لأخرى حيث بلغت (١,٢٢)، (١,٣٦)، (١,٣٧) وذلك لسنوات الدراسة من ٢٠١٩ حتى ٢٠٢١ على الترتيب، **وفيمّا يتعلق بمتوسط التزام شركات العينة بقواعد وأليات الحوكمة والذى بلغ** (٨,٠٤) في ضوء المؤشر الذى وضعه الباحث والمكون من ١٠ بنود، يلاحظ من النتائج زيادة التزام الشركات بقواعد الحوكمة من سنة لأخرى؛ حيث بلغت مؤشر التطبيق(٧,٤)، (٨,١)، (٨,٥)، وذلك لسنوات الدراسة من ٢٠١٩ حتى ٢٠٢١ على الترتيب، وهذه النسبة تعتبر هامة عند قياس العلاقة بين الإفصاح عن المخاطر السيبرانية وقيمة المنشأة،

وفى إطار توصيف متغيرات الدراسة، يوضح الجدول التالي الإحصاء الوصفي لمتغيرات الدراسة على مستوى البنوك والشركات الممثلة لقطاعات العينة وذلك كما يلى:

الجدول رقم (١٢)
الإحصاء الوصفى لمتغيرات الدراسة حسب نوع القطاع

القطاع	الإحصائيات الوصفية	نسبة الإفصاح عن المخاطر السيبرانية	قيمة المنشاة	حجم الشركة	ربحية الشركة	درجة الرفع المالى	جودة حوكمة الشركات
قطاع البنوك (٢٤ مشاهدة)	المتوسط	٠,٤٨٥	٠,٩٧٤	١٧,٩٥٩	٠,٠٢٢	٠,٨٩١	٨,٣٣٣
	الإنحراف المعيارى	٠,١٤٧	٠,٠٥٥	١,٣٣٤	٠,٠١١	٠,٠٣٦	٠,٧٦١
	أقصى قيمة	٠,٧٩٢	١,٠٩٦	٢٠,٠٢٣	٠,٠٤٧	٠,٩٩٧	١٠
	أقل قيمة	٠,٣٥٨	٠,٨٨٦	١٥,٢٨٥	٠,٠٠٣	٠,٨٥٤	٧
	التباين	٠,٠٢١	٠,٠٠٣	١,٧٧٩	٠	٠,٠٠١	٠,٥٨
شركات اتصالات واعلام وتكنولوجيا المعلومات (١٨ مشاهدة)	المتوسط	٠,٤٢٦	١,٤٣٢	٢٢,٣٥	٠,٠٦٥	١,٨٨٨	٧,٦٦٧
	الإنحراف المعيارى	٠,٢٥٩	٢,٤٧٥	١,٥٤٢	٠,٠٥٤	٠,٧٢٨	١,٠٢٩
	أقصى قيمة	٠,٩٤٣	٩,٧٣٣	٢٥,٢٣١	٠,١٨٦	٣,١٧١	٩
	أقل قيمة	٠,٢٢٦	٠,٢٣٤	٢٠,١٩٤	-٠,٠٤	١,٠٥	٦
	التباين	٠,٠٦٧	٦,١٢٥	٢,٣٧٩	٠,٠٠٣	٠,٥٣١	١,٠٥٩

المصدر: نتائج التحليل الاحصائي.

يلاحظ من الجدول السابق أن قطاع البنوك يفصح عن المخاطر السيبرانية بمتوسط (٤٨,٥٪)، ومتوسط القيمة السوقية للبنوك بلغت (٠,٩٧٤) بالاعتماد على نسبة (TOBIN Q)، كما بلغ اللوغاريتم الطبيعى لإجمالى الأصول والدال على حجم القطاع (١٧,٩٥)، بمتوسط ربحية بلغت (٠,٠٢٢)، ودرجة رفع مالى بلغت في المتوسط (٠,٨٩١)، كما بلغت مستوى جودة الحوكمة في قطاع البنوك (٨,٣) من إجمالي القيمة (١٠)، في مقابل أن شركات الاتصالات وتكنولوجيا المعلومات تفصح عن المخاطر السيبرانية بمتوسط (٤٢,٦٪)، ومتوسط القيمة السوقية للشركات بلغت (١,٤٣٢) بالاعتماد على نسبة (TOBIN Q)، كما بلغ اللوغاريتم الطبيعى لإجمالى الأصول والدال على حجم القطاع (٢٢,٣٥)، بمتوسط ربحية بلغت (٠,٠٦٥)، ودرجة رفع مالى بلغت في المتوسط (١,٨٨)، كما بلغت مستوى جودة الحوكمة في قطاع الاتصالات وتكنولوجيا المعلومات (٧,٦) من إجمالي القيمة (١٠).

٣/٢/٦- تحليل نتائج اختبار فروض الدراسة:

يتم اختبار مدى صحة الفرض الأول من خلال قياس مدى التباين في مستوى الإفصاح عن المخاطر السيبرانية بين شركات العينة (قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات)، كما يتم اختبار مدى صحة الفرض الثانى من خلال تحليل نتائج الارتباط والفرض الثالث من خلال مناقشة نتائج الانحدار وذلك كما يلى:

١- اختبار الفرض الأول: حيث ينص الفرض الأول على: يوجد تفاوت في الإفصاح الإلكتروني عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.

ويتم اختبار مدى صحة الفرض الأول من خلال قياس التمايز في مستوى الإفصاح عن المخاطر السيبرانية بين شركات العينة (قطاع البنوك وقطاع الإتصالات وتكنولوجيا المعلومات) وذلك من خلال مقارنة المتوسطات بين القطاعين على مستوى مجموعات المؤشر المقترح لقياس مستوى الإفصاح عن المخاطر السيبرانية، بالإضافة إلى تحليل نتائج إختبار Mann-Whitney لقياس التباين بين عينتين مستقلتين وهو أحد الإختبارات اللامعلمية ليتناسب مع متغير الإفصاح عن المخاطر السيبرانية والذي لاتتتبع بياناته التوزيع الطبيعى، وذلك كما يلى:

الجدول رقم (١٣)
التمايز في مستوى الإفصاح عن المخاطر السيبرانية بين قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات

القطاع	الإحصاء الوصفى لمتغيرات الدراسة حسب نوع القطاع							تحليل نتائج إختبار التباين مستوى المعنوية (SIG.) Mann-Whitney Test
	الإحصائيات الوصفية	المجموعات المكونة للمؤشر المقترح لقياس مستوى الإفصاح عن المخاطر السيبرانية					نسبة الإفصاح عن المخاطر السيبرانية ككل (%)	
		قنوات الاتصال الإلكترونية للشركة (٨) بنود	المخاطر السيبرانية الفعلية والمحتملة (١١) بند	الآثار المحتملة للمخاطر السيبرانية (٦) بنود	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (١٣) بند	تخفيف المخاطر السيبرانية (١٥) بند		
قطاع البنوك (٢٤ مشاهدة)	المتوسط	٨	٤,٣٣	١,٦٦	٦,٣٧	٥,٣٣	٠,٤٨٥	٠,٠٠٢
	الإنحراف المعيارى	٠	١,٧٦١	١,٢٧٤	٢,٧٩٥	٢,٩٢٩	٠,١٤٧	
	أقصى قيمة	٨	٩	٤	١٢	١٢	٠,٧٩٢	
	أقل قيمة	٨	٣	٠	٣	٢	٠,٣٥٨	
	متوسط الرتب	٢١,٥٠	٢٢,٦٠	٢٢,٦٩	٢٦,٥٤	٢٦,٣٨	٢٦,٤٨	
شركات اتصالات واعلام وتكنولوجيا المعلومات (١٨ مشاهدة)	المتوسط	٨	٤,٥٥	١,٧٢	٤,٤٤	٣,٨٣	٠,٤٢٦	
	الإنحراف المعيارى	٠	٢,٩٧٥	٢,٢١٨	٣,٨٢٣	٥,٠٣٢	٠,٢٥٩	
	أقصى قيمة	٨	١٠	٧	١٢	١٥	٠,٩٤٣	
	أقل قيمة	٨	١	٠	٢	٠	٠,٢٢٦	
	متوسط الرتب	٢١,٥٠	٢٠,٠٣	١٩,٩٢	١٤,٧٨	١٥,٠٠	١٤,٨٦	

المصدر: نتائج التحليل الاحصائي.

- **يتضح من الجدول السابق أن مستوى المعنوية لاختبار (Mann-Whitney Test) قيمة (٠,٠٠٢)** وهو أقل من (٠,٠٥) للتباين حول مستوى الإفصاح عن المخاطر السيبرانية، ويدل ذلك على وجود فروق معنوية بين قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات، **وفى ضوء النتيجة السابقة ووفقا لمتوسط الرتب لإختبار (Mann-Whitney) والمتوسطات الإحصائية يعد قطاع البنوك** هو الأعلى من حيث الإفصاح عن المخاطر السيبرانية من قطاع الاتصالات وتكنولوجيا المعلومات.

و**تتفق** هذه النتائج مع دراسة**(Héroux and Fortin, 2020)**، والتي توصلت إلى أن الشركات تختلف على نطاق واسع في مقدار التفاصيل التي تقدمها بشأن المخاطر السيبرانية وتخفيفها، وتوجد فروق ذات دلالة إحصائية بشأن المخاطر السيبرانية، وتخفيف المخاطر السيبرانية، وحوادث الأمن السيبراني المحتملة. وكذلك **اتفقت مع دراسة (Ramírez et al., 2022)**، والتي أشارت إلى أن أعلى نسبة إفصاح عن المخاطر السيبرانية على مستوى القطاعات، يرجع الفضل في الإفصاحات الأكثر شمولاً إلى القطاع المالي.

ويرى الباحث أن التباين بين قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات الممثلين للعينة حول الإفصاح عن المخاطر السيبرانية سببه، اختلاف خصائص الشركات لكل قطاع؛ حيث لكل شركة خصائص تميزها عن الشركة الأخرى مثل الحجم والربحية ودرجة الرفع المالى ومدى الإلتزام بالحوكمة، بالإضافة إلى عدم وجود إطار موحد تلتزم به الشركات عند الإفصاح عن المخاطر السيبرانية أو حتى تسترشد به.

وفى ضوء النتائج السابقة يخلص الباحث إلى ثبوت صحة الفرض الأول للبحث بوجود تفاوت في الإفصاح الإلكتروني عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.

٢- **تحليل نتائج اختبار الفرض الثانى، حيث ينص الفرض:** يوجد ارتباط معنوى بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشأة، ويتم اختبار هذه الفرض من خلال إعداد مصفوفة الارتباط لمتغيرات الفرض(الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشأة والمتغيرات الرقابية) وذلك كما يلي:

جدول رقم (١٤)
نتائج تحليل مصفوفة الارتباط لمتغيرات الفرض الثانى

نوع المتغير	متغيرات الفرض	قيمة المنشأة	الإفصاح الإلكتروني عن المخاطر السيبرانية	حجم الشركة	ربحية الشركة	درجة الرفع المالى	جودة حوكمة الشركات
المتغير التابع	قيمة المنشأة	١					
المتغيرات المستقلة	الإفصاح الإلكتروني عن المخاطر السيبرانية	٠,٦٧٤**	١				
		٠,٠٠٠					
المتغيرات الرقابية	حجم الشركة	٠,٠٢٩	٠,١٥٨-	١			
		٠,٤٢٨	٠,١٥٩				
	ربحية الشركة	٠,٢٩٨*	٠,١٠٩	٠,٤٣٨**	١		
		٠,٠٢٧	٠,٢٤٧	٠,٠٠٢			
	درجة الرفع المالى	٠,٥٣٦**	٠,١٨٤	٠,٦١٠**	٠,٤٣١**	١	
		٠,٠٠٠	٠,١٢٢	٠,٠٠٠	٠,٠٠٢		
	جودة حوكمة الشركات	٠,٣٦٠**	٠,٥٧٥**	٠,٤٥٣-**	٠,٢٨٢-*	٠,٠١	١
		٠,٠١	٠,٠٠٠	٠,٠٠١	٠,٠٣٥	٠,٤٧٦	

المصدر: نتائج التحليل الاحصائي.
**** تشير إلى معنوية معامل الإرتباط عند مستوى معنوية ٠,٠١**
*** تشير إلى معنوية معامل الإرتباط عند مستوى معنوية ٠,٠٥**
من الجدول السابق يتضح للباحث النتائج الأتية:

- **وجود علاقة ارتباط إيجابية معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة،** حيث أن معامل الارتباط موجب بقيمة (٠,٦٧٤) ومستوي المعنوية (sig) بلغ (٠,٠٠٠) أقل من (٠,٠١)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى تحسن في القيمة السوقية للشركة في السوق، **مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة إرتباط معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة.**
- **بالنسبة للمتغيرات الرقابية** والتي يتم أخذها في الاعتبار عند الحكم على العلاقة بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة، أكدت نتائج الجدول السابق على وجود علاقة موجبة معنوية بين كل من ربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات وبين قيمة المنشأة، بينما ارتبطت حجم الشركة بعلاقة غير معنوية مع قيمة المنشاة.

ويخلص الباحث مما سبق أنه فى ضوء ضوابط العينة المختارة فأنه كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى تحسن في قيمة الشركة، **وبالتالي ثبوت صحة الفرض الثانى للدراسة بوجود علاقة إرتباط معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة.**

وهذه النتيجة **تتفق مع دراسة(Cheong, 2021, p36)**، والتي أشارت إلى أن الإفصاح عن المخاطر السيبرانية المعدل بمستوى الصناعة CRDS وهو يساوي إجمالي(FS_CRDS+IL_CRDS), حيث يتفاعل السوق بشكل إيجابي مع الإفصاح الإجمالي عن المخاطر السيبرانية، وبلغ مستوى المعنوية(٦,٩٨٥*)، ويتفاعل بشكل إيجابي مع المخاطر السيبرانية الخاصة بالمنشأة، وبلغ معامل(FS_CRDS)الخاصة بالشركات(٢٣,٢٧٤)، وهو أمر إيجابي ودال إحصائياً(٣,٧١٩*) عند p <0.001، وهذا يدعم الحجة القائلة بأن الإفصاح عن المخاطر السيبرانية الخاصة بالمنشأة ذات صلة بالقيمة، وتستجيب المنشأة التي تفصح عن المخاطر السيبرانية بشكل أفضل مقارنةً بالشركات الأخرى.

٣- تحليل نتائج اختبار الفرض الرئيسى الثالث، حيث ينص الفرض الثالث: يوجد أثر ذو دلالة إحصائية للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة.

ولقياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة، قام الباحث بتحليل الإنحدار بشكليه **البسيط** في ظل عدم وجود المتغيرات الرقابية، **والمتعدد** في ظل إدخال المتغيرات الرقابية، **ويعرض الجدول التالى نتائج الانحدار كما يلى :**

جدول رقم (١٥)

نتائج تحليل الانحدار بين متغيرات الفرض الثالث

المتغيرات المستقلة فى النموذج (مستقلة ورقابية)	نتائج تحليل الإنحدار قبل وبعد إدخال المتغيرات الرقابية (أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة)						
	النموذج	التحليل الأساسى			التحليل الإضافى (وجود المتغيرات الرقابية)		
	العلاقة المستهدفة	أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة			أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة في ظل وجود المتغيرات الرقابية		
	الرمز	قيمة B	قيمة T	Sig.	قيمة B	قيمة T	Sig.
المقدار الثابت	B_0	١,٣٠٠-	٢,٧٨٦-	٠,٠٠٨	٢,٢٦٥	٠,٧٨٩	٠,٤٣٥
الإفصاح الإلكتروني عن المخاطر السيبرانية	CRD	٥,٣٧٤	٥,٧٧١	٠,٠٠٠	٠,٠٨٢	٤,٤٤٧	٠,٠٠٠
حجم الشركة	FSIZE	-	-	-	٠,٢٠٢	٢,٢٣١	٠,٠٣٢
ربحية الشركة	ROA	-	-	-	٤,٠٦٨	٠,٩١٢	٠,٣٦٨
درجة الرفع المالى	LEV	-	-	-	١,٣٨٨	٤,٣١٦	٠,٠٠٠
جودة حوكمة الشركات	CGQ	-	-	-	٠,١٣٦	٠,٥٥٧	٠,٠٨١
القيمة التفسيرية (R^2)		معامل التحديد R^2 = ٠,٤٥٤			معامل التحديد R^2 = ٠,٦٨٠		
قيمة F		قيمة F٣٣,٣٠٩ =			قيمة F١٥,٢٩٠ =		
المعنوية الكلية للنموذج		مستوى (SIG.) = ٠,٠٠٠			مستوى (SIG.) = ٠,٠٠٠		

المصدر: نتائج التحليل الاحصائي.

وبالنظر لكل نموذج بشكل مستقل يتضح للباحث ما يلي:

- **بالنسبة للمعنوية الكلية لنماذج الانحدار** التي تمثل الفرض الثالث للدراسة على مستوى التحليل الأساسى والإضافي من خلال تحليل التباين (**ANOVA**) للنموذج ككل، بلغت مستوى المعنوية (٠,٠٠٠)، وهي أقل من (٠,٠٥) مما يدل على ارتفاع معنوية النموذج المستخدم وصلاحيته لتحقيق هدف الدراسة.
- **أن قيمة معامل التحديد (R^2) لنموذج الانحدار**، قبل إدخال المتغيرات الرقابية وبعد إدخالها تبلغ (٠,٤٥٤)، (٠,٦٨٠) على الترتيب وهي قيمة تعكس درجة تفسير المتغيرات المستقلة للتغيرات التي تحدث في المتغير التابع في كل نموذج، حيث يفسر الإفصاح عن المخاطر السيبرانية بمفرده التغيرات التي تحدث في المتغير التابع (قيمة المنشأة) بنسبة ٤٥,٥٪، بينما تفسر المتغيرات المستقلة (الإفصاح عن المخاطر السيبرانية والمتغيرات الرقابية) التغيرات التى تحدث فى المتغير التابع (قيمة الشركة) بنسبة ٦٨٪ بينما ترجع باقى التغيرات في كل حالة إلى أسباب ومتغيرات أخرى خارج الدراسة ولم يتناولها الباحث.
- **وجود أثر إيجابي ذو دلالة إحصائية عند مستوى معنوية (٠,٠١) للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها وهى** (حجم الشركة، ربحية الشركة، درجة الرفع المالى وجودة الحوكمة)، حيث أن معامل الإنحدار موجب ومستوي المعنوية (sig) أقل من (٠,٠١).

ويقدم هذا دليلاً على الضوء الإيجابي على المخاطر النظامية المتعلقة بالأمن السيبراني بقدر ما يتم تحفيز السوق والمنشأة نفسها على دمج هذه التأثيرات في أسعار الأصول، حيث أن تقييم الإدارة للمخاطر السيبرانية، يعزز قدرة المنشأة على الإستجابة وتقليل عدم تناسق المعلومات، ويجبر الإدارة على أن يكون لديها استراتيجيات طارئة، مما يؤدي إلى التقييم العادل لهذه المخاطر Histen , 2022, p1, 3,

(5, 11).وجاءت هذه النتيجة متوافقة مع دراسة(Chen et al., 2022, p8-9)، والتي أكدت على أنه عندما تتضمن محتوى الإفصاحات المتزايدة تدابير إضافية لمنع المخاطر، فمن المحتمل أن يكون رد فعل السوق إيجابياً، ويحدث رد فعل سلبي كبير في السوق إذا قللت الشركات المخترقة من الإفصاح عن المخاطر السيبرانية. وكذلك اتفقت مع دراسة(Tayaksi et al., 2022, p659-661)، والتي توصلت إلى أنه لوحظ تأثير إيجابي لقطاع الاتصالات في جميع نوافذ الحدث، وتم فحص نتائج النموذج CAR المعدل بالسوق والنموذج المتوسط المعدل CAR بالإضافة إلى نموذج السوق CAR، ومع ذلك، فإن نتائج جميع النماذج متسقة ولا يُظهر أي من النماذج في قطاع الاتصالات تأثيراً سلبياً كبيراً، حيث أن هناك ثقة عالية بالفعل في قطاع الاتصالات وأن القطاع يدير الأيام السابقة واللاحقة للإعلان عن الأحداث بفعالية.

وتشير الدراسات التجريبية الحديثة إلى أنه ليست كل التأثيرات سلبية، على سبيل المثال، فقد أشار (Gay, 2017) إلى أن بعض المؤسسات قد تشهد زيادة في عوائد سوق الأسهم بسبب التغطية الإعلامية الإيجابية بعد حدث الاختراق. ووجدت دراسة(Rosati et al., 2022)أن هذه الإعلانات لها تأثير إيجابي قصير المدى على حجم التداول في يوم الحدث، ولا توجد تأثيرات على اليوم السابق للحدث، ثم تعود بسرعة إلى الحالة الطبيعية بعد يوم الحدث. ولم تؤكد دراسة(Juma'h and Alnsour, 2021, p13) على وجود علاقة جوهرية بين خروقات البيانات ورد فعل سوق الأسهم عند حدوث إختراق سيبراني، وقد يتفاعل المستثمرون في أسواق الأسهم مع إعلانات خرق البيانات بشكل يومي وليس على أساس ربع سنوي. ومع ذلك عندما تتعرض الشركة لهجمات سابقة ، قد يدرك المستثمرون أن خطر الهجوم السيبراني أعلى بالنسبة لمثل هذه الشركة، مما يؤدي إلى علاوة أعلى في أسعار الأسهم للإفصاح عن الاستراتيجية المخففة (Cao et al., 2023, p6081).

- **وجود اثر إيجابى لكل من ربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات على قيمة المنشأة، بينما أكدت نتائج الجدول على عدم وجود أثر معنوى لحجم الشركة علي قيمة المنشاة.**

وتتفق هذه النتيجة مع دراسة**(Tong, 2023, p7, 10)**، والتي توصلت إلى أن سعر سهم الشركة بشكل عام يتأثر أكثر بالعائد على الأصول ROA، والرافعة المالية ومؤشرات التشغيل التقليدية الأخرى للشركة، ومستوى المعنوية(P-value) هي ٠,٠٠٣، وهي ذات دلالة إحصائية عند مستوى ١٪.

وفى ضوء نتائج الإنحدار المتعدد لقياس العلاقة بين الإفصاح الإلكترونى للمخاطر السيبرانية وقيمة المنشاة فى ظل وجود المتغيرات الرقابية، يمكن تكوين معادلة كمية، كما يلي:

$$FV = 2.265 + 0.082\ (CRD) + 0.202\ (FSIZE) + 4.068\ (ROA) + 1.388\ (LEV) + 0.136\ (CGQ) + \varepsilon it$$

حيث (**FV**): قيمة المنشأة، **CRD**: الإفصاح الإلكترونى عن المخاطر السيبرانية، (**FSIZE**) هو حجم الشركة، (**ROA**) ربحية الشركة الشركة، (**LEV**) درجة الرفع المالى للشركة،(**CGQ**) جودة حوكمة الشركات.

وبعد تناول الباحث لنتائج الإنحدار يخلص الباحث إلى ثبوت صحة الفرض الثالث للدراسة والذي ينص على " يوجد أثر ذو دلالة إحصائية للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة **"**.

سابعاً: النتائج والتوصيات والدراسات المستقبلية.

استهدف البحث دراسة وقياس أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها على مؤشرات قيمة المنشأة، ويمكن بلورة أهم نتائج البحث بشقيه النظري والتطبيقي، على النحو التالي:

١- في ظل السعي لوضع تعريف وصياغة مفهوم للمخاطر السيبرانية، يري الباحث أنها عبارة عن مدى تعرض الوحدة الاقتصادية لخسائر(مالية وغير مالية)واسعة النطاق، وغير متوقعة ونتائج غير مرغوب فيها، نتيجة حدوث تهديدات محتملة غير مؤكدة للإضرار بسرية ونزاهة وتوافر البيانات والمعلومات الخاصة في الفضاء السيبراني، مما يؤثر على قدرتها على تحقيق أهدافها واستمراريتها في حالة وقوع هذه المخاطر.

٢- استخلصت الدراسة النظرية أن قيمة المنشأة في البيئة الرقمية تعبر عن القيمة الحقيقية الفعلية للأصول في السوق، ومدى قدرة إدارة المنشأة في خلق منافع اقتصادية مستقبلية تساوي أو أكبر مما هو متوقع، من خلال الاستغلال الأمثل للموارد والفرص المتاحة في الأجلين القصير والطويل، وحماية أصولها من أي مخاطر وتهديدات سيبرانية حالية أو متوقعة في الفضاء السيبراني المحيط بالمنشأة، ووضع سيناريوهات واجراءات واضحة للتعامل مع أي أزمة أو ظروف طارئة قد تحدث بمرور الزمن.

٣- يعتمد رد فعل السوق على التغيرات في الإفصاح بالزيادة أو الانخفاض عن المخاطر السيبرانية بعد خرق البيانات، واتضح للباحث أهمية دراسة وتحليل أثر الإفصاح عن المخاطر السيبرانية على القيمة السوقية في الشركات المدرجة بالبورصة المصرية، نظراً لأنه لا يوجد حتي الآن- في حدود علم الباحث- أيه دراسة عربية أو مصرية، تناولت هذه العلاقة، كما توقع الباحث أن ردود فعل السوق ستختلف بين القطاعات، حيث يكون تأثير الاختراق الأمني أعلى في بعض القطاعات عن القطاعات الأخرى.

٤- خلصت نتائج الدراسة التطبيقية، إلى وجود تفاوت في الإفصاح الإلكتروني عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات، **حيث بلغت قيمة اختبار (Mann-Whitney Test) (٠,٠٠٢)** وهو أقل من (٠,٠٥) للتباين حول مستوى الإفصاح عن المخاطر السيبرانية، ويدل ذلك على وجود فروق معنوية بين قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات، **ووفقا لمتوسط الرتب لإختبار (Mann-Whitney) والمتوسطات الإحصائية، يعد قطاع البنوك** هو الأعلى من حيث الإفصاح عن المخاطر السيبرانية من قطاع الاتصالات وتكنولوجيا المعلومات.

٥- **وجود علاقة ارتباط إيجابية معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة،** حيث أن معامل الارتباط موجب بقيمة (٠,٦٧٤) ومستوي المعنوية (sig) بلغ (٠,٠٠٠) أقل من (٠,٠١)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى تحسن في القيمة السوقية للشركة في السوق، **مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة إرتباط معنوية بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة، وبالنسبة للمتغيرات الرقابية** والتي تم أخذها في الاعتبار عند الحكم على العلاقة بين الإفصاح الإلكتروني عن المخاطر السيبرانية وقيمة المنشاة، **أكدت نتائج الدراسة التطبيقية،** على وجود علاقة موجبة معنوية بين كل من ربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات وبين قيمة المنشأة، بينما ارتبط حجم الشركة بعلاقة غير معنوية مع قيمة المنشاة.

٦- **وجود أثر إيجابى ذو دلالة إحصائية عند مستوى معنوية (٠,٠١) للإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشاة وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها وهى** (حجم الشركة، ربحية الشركة، درجة الرفع المالى، وجودة الحوكمة)، حيث أن معامل الإنحدار موجب ومستوي المعنوية (sig) أقل من (٠,٠١)، **وبالنسبة للمتغيرات الرقابية، أكدت نتائج الدراسة التطبيقية،** وجود اثر إيجابى لكل من ربحية الشركة ودرجة الرفع المالى وجودة حوكمة الشركات على قيمة المنشأة، بينما أكدت النتائج على عدم وجود أثر معنوى لحجم الشركة علي قيمة المنشاة.

واستناداً إلى ما توصل إليه البحث من نتائج، يقدم الباحث مجموعة من التوصيات التالية:

١- ضرورة التحقق من جودة الإفصاح الالكتروني عن المخاطر السيبرانية، وأن يتضمن الإفصاح الالكتروني معلومات ذات قيمة لمتلقيها، لمساعدة أصحاب المصلحة على اتخاذ القرارات بعد حدوث

الخرق الأمني، وتتعلق بوصف مصادر التهديد والغرض منه، وطبيعة الأحداث والآثار المحتملة والحل المحتمل.

٢- ضرورة تبني الشركات المدرجة بالبورصة المزيد من الافصاح الشفافية في التقارير والقوائم المالية، لإعلام مستثمريها بكافة المخاطر السيبرانية المحتملة والفعلية الجوهرية، التي قد تؤثر على أعمالها ونتائجها المالية، والإفصاح عن سيناريوها مواجهة المخاطر السيبرانية وإدارتها، والتخفيف من حدتها.

٣- ينبغي أن تكون لدى المنشآت سياسات وضوابط أمنية كافية، لتمكين الإفصاح الداخلي عن المشاكل الأمنية؛ بحيث يتم إبلاغ الإدارة العليا ومجلس الإدارة بشفافية، وأن تسعى الإدارة العليا إلى الإشارة لمسؤوليتها تجاه أصحاب المصلحة، وذلك لتحقيق مجالات جودة الإفصاح عن المخاطر السيبرانية الثلاثة، (الاكتمال وحسن التوقيت ومدى مشاركة الإدارة عموماً في عملية الإفصاح عن المخاطر السيبرانية).

٤- إصدار معيار محاسبي لتنظيم القياس والافصاح عن المخاطر السيبرانية، وآثاها المحتملة على الفروض والمبادئ المحاسبية وعلى القوائم والتقارير المالية، واصدار قانون ملزم للشركات المقيدة بالبورصة للإفصاح عن المخاطر السيبرانية وبرامج إدارتها، أسوةً بالبورصة الأمريكية وبورصة تورنتو والاتحاد الأوروبي والصين، حيث أصبحت ضرورة ملحة في الوقت الراهن، خاصةً وأن مصر تتعرض لهجمات سيبرانية مرتفعة في الوقت الحالي، ولكي تتواكب المعايير والتعليمات مع رؤية مصر ٢٠٣٠، والتطورات في البيئة الرقمية ورقمنة وأتمتة المحاسبة، وينبغي على البنك المركزي المصري اصدار ونشر استراتيجية وتعليمات رقابية لكافة البنوك المصرية الخاضعة لرقابته، بتنظيم الافصاح عن المخاطر السيبرانية، ومحاولة التحوط من هذه المخاطر، والتعاون مع شركات التأمين بإصداروثائق تأمين ضد هذه المخاطر، واصدار تعليمات للمرونة والحوكمة السيبرانية.

وأخيراً، يقترح الباحث بعض المجالات للبحوث المستقبلية، والتي يمكن أن تشمل ما يلي:

١- أثر الإفصاح عن المخاطر السيبرانية على جودة التقارير المالية وإنعكاس ذلك على ترشيد قرارات المستثمرين.

٢- أثر القياس والإفصاح المحاسبي عن المخاطر السيبرانية على البيع على المكشوف وإنعكاس ذلك على الاستقرار المالي للبنوك التجارية المقيدة بالبورصة المصرية.

٣- الدور المرتقب للمراجع الخارجي في إدارة المخاطر السيبرانية وإنعكاس ذلك على جودة المراجعة المدركة.

٤- أثر القياس والإفصاح المحاسبي عن المخاطر السيبرانية على الخسائر الائتمانية المتوقعة وإنعكاس ذلك على المرونة السيبرانية في ضوء معايير IFRS والتعليمات الرقابية للجنة بازل دراسة تطبيقية على البنوك التجارية المقيدة بالبورصة المصرية.

قائمة المراجع

أولاً: المراجع العربية:

- **الكتب:**

١- سليمان، أسامة ربيع أمين.(٢٠٠٧). التحليل الإحصائي باستخدام برنامج SPSS الجزء الأول مهارات أساسية اختبارات الفروض الإحصائية (المعلمية – اللامعلمية).، مكتبة الأنجلو المصرية، القاهرة، ص ١١٥- ١٩٧.

٢- الزغبى، محمد بلال، الطلاحفة، عباس.(٢٠١٢).النظام الإحصائى spss فهم وتحليل البيانات الإحصائية" الجامعة الأردنية، الأردن، الطبعة الثالثة، ص ٣١٤.

- **المجلات والدوريات العلمية:**

١- أبو الخير، محمد حارس محمد طه. (٢٠٢٣). أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية). المجلة العلمية للدراسات والبحوث المالية والإدارية, كلية التجارة، جامعة مدينة السادات، المجلد ١٥، العدد الأول، مارس، ص١-٧١.

٢- الامبابي، محمد عبد الحميد أحمد الإمبابي. (٢٠٢٢). قياس وتقدير مخاطر (Covid-19) على سوق الأوراق المالية المصري باستخدام القيمة المعرضة للخطر(VAR) . المجلة العلمية للبحوث التجارية، كلية التجارة، جامعة المنوفية، المجلد ٤٥، العدد ٢، أبريل، ص٥٧٥-٦٠٢.

٣- الأمير، شمران عبيد خليف. (٢٠٢٢). أثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني . مجلة الكوت للعلوم الإقتصادية و الإدارية، كلية الإدارة والإقتصاد، جامعة واسط، المجلد١٤، العدد ٤٥، ص٤٨٦-٥٠٣.

٤- الباز، محمد ماهر عبد الحميد.(٢٠٢٢). تأثير التحفظ المحاسبي على العلاقة بين مستوى الاحتفاظ بالنقدية وقيمة الشركة - دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية. مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، المجلد ٢٦، العدد ١، إبريل ٢٠٢٢، ص ٦٣- ١١٤.

٥- الرشيدي، طارق عبد العزيز، عباس، داليا عادل. (٢٠١٩). أثر الإفصاح عن مخاطر الأمن السيبرانى في التقارير المالية على أسعار الأسهم وأحجام التداول : دراسة مقارنة في قطاع تكنولوجيا المعلومات. مجلة المحاسبة والمراجعة، كلية التجارة، جامعة بني سويف، المجلد ٨، العدد الثاني، ص٤٣٩- ٤٨٧.

٦- السواح، نادر شعبان إبراهيم. (٢٠٢١). انعكاس جائحة كورونا على نظم الرقابة الداخلية وأثرها على أمن المعلومات بالبنوك التجارية المصرية: دراسة ميدانية .مجلة التجارة والتمويل، كلية التجارة، جامعة طنطا، ع١، ص٤٧٣-٥٣٦.

٧- الصاوي، عفت أبو بكر محمد. (٢٠٢٢). أثر الإفصاح المحاسبي عبر الإنترنت ووسائل التواصل الاجتماعي علي تكلفة رأس المال في ظل عدم التماثل في المعلومات بالتطبيق على الشركات المقيدة بالبورصة المصرية. مجلة الاسكندرية للبحوث المحاسبية, كلية التجارة، جامعة الاسكندرية، ٦(٢), ٣٥-١١٢.

٨- الصيرفي، أسماء أحمد.(٢٠٢٢). أثر تطبيق الشركات لإدارة مخاطر الأمن السيبراني علي جودة المراجعة الخارجية". المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة- تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين،(١٠-١١ مارس٢٠٢٢)، كلية التجارة، جامعة الإسكندرية، ص ١-١١.

٩- القليطي، إبراهيم عبد المجيد على.(٢٠١٩). تأثير الإفصاح عن المخاطر على القيمة السوقية للشركة- دراسة تطبيقية على الشركات المدرجة بالبورصة المصرية، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الإسكندرية، المجلد الثالث، العدد الثاني، ص١-٧٣.

١٠-أميرهم، جيهان عادل ناجى أميرهم. (٢٠٢٢). اثر جودة المراجعة الداخلية فى الحد من مخاطر الامن السيبرانى و انعكاساته على ترشيد قرارات المستثمرين (دارسة ميدانية). مجلة البحوث المالية والتجارية, كلية التجارة، جامعة بورسعيد، المجلد ٢٣، العدد الثالث، يوليو، ص ٣٢٥-٣٧٧.

١١-بيومي، ميهاب صلاح. (٢٠٢١). قياس أثر مستوى الإفصاح بالتقارير السردية على قيمة الشركة دراسة تطبيقية على سوق الأوراق المالية المصري .المجلة العلمية للدراسات التجارية والبيئية، كلية التجارة، جامعة قناة السويس، ١١(العدد الثاني، الجزء الثاني), ١٣٥٠-١٣٧٣.

١٢-جبر، غريب جبر.(٢٠٢٢). تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها. المؤتمر العلمي السنوي لقسم التمويل والمحاسبة، الخدمات البنكية في ظل ابتكارات التكنولوجيا المصرفية(الفرص والتحديات)، (٢٣مايو٢٠٢٢)، الأكاديمية الدولية للهندسة وعلوم الإعلام، المجلد الأول، العدد الأول.

١٣-حماده، نورا عبدالصمد، مهنى، شيماء فكري.(٢٠٢٢). أثر تطبيق آليات الحوكمة على العلاقة بين مستوى الإفصاح الإلكتروني وقيمة الشركة "دراسة اختبارية على الشركات المساهمة المصرية"، مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق، المجلد الرابع والأربعون، العدد الثالث، ص٤١-٨٢.
١٤-شحاتة، محمد موسي علي، والبردان، محمد فوزي أمين.(٢٠٢١). أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل استراتيجيات الرقمنة على الحد من المخاطر السيبرانية"، المؤتمر الدولي الثالث، الرقمنة وضمان جودة التعليم العالي، جامعة مدينة السادات، ٢-٣ أكتوبر ٢٠٢١، ص١-٢٥.
١٥-شرف، إبراهيم أحمد إبراهيم.(٢٠٢٣). أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين - دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، قسم المحاسبة والمراجعة، كلية التجارة، جامعة الاسكندرية، العدد الاول، المجلد السابع، ص٢١١-٢٨٢.
١٦-صالح، نرمين محمد شاكر إبراهيم.(٢٠٢٢). محددات فعالية المراجعة الداخلية للأمن السيبراني". المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة- تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين،(١٠-١١ مارس٢٠٢٢)، كلية التجارة، جامعة الإسكندرية، ص ١-٢٤.
١٧-عازر، رانيا هاني رمزي.(٢٠٢٢). قياس أثر الإفصاح المحاسبي عن خسارة اضمحلال الشهرة على تكلفة رأس المال وقيمة الشركة: دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية. مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية، كلية التجارة، جامعة بني سويف، المجلد ١١، العدد ٣، ديسمبر ٢٠٢٢، ص٣٣-٧١.
١٨-عثمان، محمد أحمد. (٢٠٢٢). محددات فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، كلية التجارة، جامعة الإسكندرية، ص ١-١٨.
١٩-عفيفي، هلال عبد الفتاح، فودة، السيد أحمد، عبده، نبيل محمد الشحات.(٢٠٢١). أثر أبعاد المسئولية الاجتماعية للشركات على تكلفة حقوق الملكية وقيمة الشركة- دراسة اختبارية، مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق، المجلد الثالث والأربعون، العدد الثاني، ص١٨٧-٢٥٠.
٢٠-عقل، يونس حسن، زهري، علاء فتحي. (٢٠٢٠) . تطوير الإفصاح المحاسبي عن الرقمنة المصرفية لتعزيز جودة التقارير المالية للبنوك العاملة في البيئة المصرية : دراسة تطبيقية. المجلة العلمية للبحوث والدراسات التجارية، كلية التجارة وإدارة الأعمال، جامعة حلوان، المجلد ٣٤، العدد الرابع، ص ٢٠١-٢٦٢.
٢١-على، عايدة محمد مصطفى. (٢٠٢٢). أثر مستوى الإفصاح عن مؤشرات الرقمنة على عدم تماثل المعلومات: دراسة تطبيقية على البنوك التجارية المقيدة بالبورصة المصرية .مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، المجلد التاسع، العدد الثاني، ص ٤٢٢-٤٩٥.
٢٢-علي، محمود أحمد أحمد، علي، صالح علي صالح. (٢٠٢٢). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية. المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة- تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين،(١٠-١١ مارس٢٠٢٢)، كلية التجارة، جامعة الإسكندرية، ص ١-٦٤.
٢٣-فرج، هاني خليل. (٢٠٢٢). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني الاستثمار بالأسهم - دراسة تجريبية. مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية، كلية التجارة، جامعة بني يوسف، المجلد ١١، العدد ٢، أغسطس، ص ١٢٩- ٢٠٩.
٢٤-كريمة، دينا عبد العليم. (٢٠٢٣). دراسة أثر القياس والإفصاح المحاسبي عن الأصول الفكرية على قيمة الشركة بالتطبيق على شركات الاتصالات وتكنولوجيا المعلومات في مصر. المجلة العلمية للدراسات والبحوث المالية والتجارية، كلية التجارة، جامعة دمياط، ٤(١)٢،٩٧٩-١٠٣٧.
٢٥-محروس، رمضان عارف رمضان, أبو الحمد، مصطفى صالح. (٢٠٢٢). استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني. مجلة البحوث المالية والتجارية, كلية التجارة، جامعة بورسعيد ، المجلد ٢٣، العدد الثالث، يوليو، ص٤٣٢-٤٩١.
٢٦-يعقوب، ابتهاج إسماعيل، وهاب، اسعد محمد علي، و الفرطوسى، علي سموم. (٢٠٢٢). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية وفق المتطلبات الدولية: دراسة اختبارية. مجلة الدراسات المالية والمحاسبية والإدارية، كلية الإدارة والإقتصاد، جامعة المستنصرية، مج٩, ع١، ص ١٤٠٣- ١٤٣٠.

٢٧-يوسف، امانى احمد وهبه. (٢٠٢٢). واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة: دراسة تطبيقية .المجلة العلمية للدراسات التجارية والبيئية، كلية التجارة، جامعة قناة السويس، المجلد ١٣، العدد ٢، إبريل، ص ٢٨- ١٠٩.

- **المواقع الإلكترونية والنشرات:**

١- البنك المركزي المصري (٢٠١٩). تقرير الاستقرار المالي لعام ٢٠١٨.
٢- البنك المركزي المصري.(٢٠٢١). التعليمات الرقابية لإدارة مخاطر التشغيل وفقاً لإصلاحات بازل ٣ الصادرة في ديسمبر ٢٠١٧، قطاع الرقابة والإشراف، ٤ يناير ٢٠٢١، ص١-٢٤.
٣- البنك المركزي المصري.(٢٠٢١). تعليمات خطط التعافي. قطاع الرقابة والإشراف، ٢ سبتمبر ٢٠٢١، ص١-١٢.
٤- البنك المركزي المصري.(٢٠٢١). الفصل الثاني القواعد المنظمة لتقديم الخدمات المصرفية عبر الإنترنت. ٩ نوفمبر ٢٠١٩، ص١-٣٦.
٥- المركز المصري للدراسات الاقتصادية.(٢٠١٩). سلسلة ورش عمل بعنوان " أجندة بحثية تفصيلية لدعم الجهة الحكومي التحول الرقمي للاقتصاد المصري - بحث ودراسة الحالة المصرية: قضايا أفقية"، الورشة الثالثة، فبراير.
٦- موقع معلومات مباشر مصر: https://www.mubasher.info/countries/EG
٧- موقع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات https://www.egcert.eg/ar/

ثانياً: المراجع الأجنبية:

- **Books:**

1- Abu-Bader, S. H. (2021). Using statistical methods in social science research: With a complete SPSS guide. Oxford University Press, USA.
2- Boban, M. (2018). Cyber security foundations for compliance within gdpr for business information systems. Economic and social development: book of proceedings, 541-553.

- **Theses:**

1- Asauri, Z. A. F. (2022). Disclosure of Cyber Risk: Its Effect on Banking Profitability in Indonesia (Doctoral dissertation, STIE Indonesia Banking School).
2- MIele, B. (2022). Modelli quantitativi per la valutazione del cyber risk. Doctoral Thesis of Department of Economics and Finance. for Finance Computational tools for finance. http://tesi.luiss.it/33248/
3- Navarro Vekez, P. (2019). Three Studies on Cybersecurity Disclosure and Assurance. (Doctoral dissertation, in the Kenneth G. Dixon School of Accounting in the College of Business Administration at the University of Central Florida Orlando, Florida).
4- Poddar, P. (2023). Internal Auditing in a digitalised world: A qualitative study about the internal auditor´ s approach in providing assurance of cybersecurity .Master Thesis in Accounting and Financial Management Specialisation. Department of Business Studies Uppsala University.
5- Schuurman, R. (2020). The effects of data breaches on the stock price in the period 2016-2018.(Doctoral dissertation of Economics). Business Economics, Erasmus University Rotterdam, Rotterdam.
6- Viancourt, P. E. (2021). Data Breach Announcements: Evaluating the Content and Timing Of Breach Announcements and Their Effect On Firm Value. Dissertations from the Executive Doctorate in Business. Rollins College.

- **Periodicals:**

1- AKÇAKANAT, Ö., ÖZDEMİR, O., & MAZAK, M. (2021). Cyber Security Risks in Businesses and Information Technology Audit: An Investigation of Banks' Cyber Security Practices. Mehmet Akif Ersoy University Journal of Applied Sciences, 5(2), 246-270.

2- Ali, S. E. A., & Lai, F. W. (2022). Cyber Security Breaches and the Long-Run Effect on Firms' Market Value: A Conceptual Framework. In International Conference on Artificial Intelligence for Smart Community (pp. 689-697). Springer, Singapore.

3- Ali, S. E. A., Lai, F. W., Aman, A., Saleem, M. F., & Hamad, S. (2022). Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk?. JOURNAL OF COMPETITIVENESS, 14(1), 23-42.

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

5- Auman, J. (2018). Hacking Our Securities Disclosure System: The Need for Federal Broker-Dealer Disclosure Requirements Vis-a-Vis Cyber Incidents. Colum. Bus. L. Rev., 952.

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

7- Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., & Vigne, S. (2023). Are the good spared? Corporate social responsibility as insurance against cyber security incidents. Risk Analysis, 1–16.

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

9- Benaroch, M. (2021). Third-party induced cyber incidents—much ado about nothing?. Journal of Cybersecurity, 7(1), tyab020.

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

11- Bricker, W., Hamm, K ., Golden, R., & Cosper, S., . (2022).Monitoring Risk in Financial Reporting Regulators Look Closer at Cybersecurity, Sustainability, and Governance Highlights from The 20th Annual Financial Reporting Conference was hosted virtually by Baruch College on May 4 and 5, 2022.

12- Cao, R., Kafaee, Ö., Aziz, A., & Cavusoglu, H. (2023). Market Reaction to Cyber Strategy Disclosure: Word Embedding Derived Approach. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. p6078-6087.

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

14- Cheong, A. (2021). If you cannot measure it, you cannot manage it: three essays on cybersecurity risk assessment (Doctoral dissertation, Rutgers University-Graduate School-Newark).

15- Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. Journal of information Systems, 35(2), 179-194.
16- Chong, W. F., Feng, R., Hu, H., & Zhang, L. (2022). Cyber Risk Assessment for Capital Management. arXiv preprint arXiv:2205.08435.
17- Cortez, E. K., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. European Journal of Risk Regulation, 13(3), 443-463.
18- Cram, W. A., Wang, T., & Yuan, J. (2022). Cybersecurity research in accounting information systems: A review and framework. Journal of Emerging Technologies in Accounting.
19- Desyatnyuk, O., Muravskyi, V., Shevchuk, O., & Oleksiiv, M. (2022, September). Dual Use of Internet of Things Technology in Accounting Automation and Cybersecurity. In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 360-363). IEEE.
20- Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking.
21- Dong, T., Zhu, S., Oliveira, M., & Luo, X. R. (2022). Making better IS security investment decisions: discovering the cost of data breach announcements during the COVID-19 pandemic. Industrial Management & Data Systems, (ahead-of-print).
22- Duvenhage, F., Smit, A., & Botha, M. (2022). Cyber Security disclosure in the banking sector: A case of South Africa and China. IBC, 1-21.
23- Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current Issues in Auditing, 13(2), C1-C9.
24- Ebrahimi, S., & Eshghi, K. (2022). A meta-analysis of the factors influencing the impact of security breach announcements on stock returns of firms. Electronic Markets, 1-24.
25- Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cyber security in Dutch annual reports of listed companies. Computer Law & Security Review, 40, 105513.
26- Eling, M., & Jung, K. (2022). Heterogeneity in cyber loss severity and its impact on cyber risk measurement. Risk Management, 1-25.
27- Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?. European Journal of Operational Research, 272(3), 1109-1119.
28- Ferens, A. (2021). Cybersecurity and cybersecurity in integrated reports and management reports of operators of key services. Accounting Theoretical Journals, (45 (2)), 31-50.
29- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351-407.
30- Gaidosch, T., Adelmann, F., Morozova, A., & Wilson, C. (2019). Cybersecurity risk supervision. Departmental Papers, 2019(014).
31- Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468.
32- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 89, 725–763.

33- Ghosh, K. (2020). Identification and Quantification of Cybersecurity Risk by Likelihood-Severity, Incident-Response and Organizational Asset Valuation Framework. Incident-Response and Organizational Asset Valuation Framework (June 18, 2020).
34- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34(5), 509-519.
35- Grove, H., Clouse, M., & Schaffner, L. G. (2019). Cybersecurity description and control criteria to strengthen corporate governance. Journal of Leadership, Accountability and Ethics, 16(1), 86-96.
36- Hapsoro, D., & Bahantwelu, M. I. (2020). Does earning management mediate the effect of capital structure on company value?. Jurnal Ekonomi dan Bisnis, 23(1), 53-68.
37- Hartmann, C. C., & Carmenate, J. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. Current Issues in Auditing, 15(2), A9-A23.
38- Hasan, M. F., & Al-Ramadan, N. S. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. Soc. Sci. Humanit. J, 5(8), 2312-2323.
39- Heidenborg, E., & Lappalainen, L. E. (2021). Cyber Risk Reporting of Large International Electric Utility Companies.
40- Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. Accounting Perspectives, 19(2), 73-100.
41- Histen, M. J. (2022). Taking Information Seriously: A Firm-side Interpretation of Risk Factor Disclosure. International Advances in Economic Research, 1-13.
42- Hussein, A., & Nounou, G. (2022). The impact of internet financial reporting on Egyptian company's performance. Journal of Financial Reporting and Accounting, 20(5), 841-865.
43- Igor, A., Igor, A., & Yurii, M. (2022). ASPECTS OF PROTECTION AND STORAGE OF ACCOUNTING INFORMATION AND CYBER SECURITY OF ENTERPRISE DATA. EDITORIAL BOARD, 965.
44- Islam, M. S., Wang, T., Farah, N., & Stafford, T. (2022). The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. Journal of Accounting and Public Policy, 41(2), 106916.
45- Janvrin, D. J., & Wang, T. (2021). Linking cybersecurity and accounting: An event, impact, response framework. Accounting Horizons (forthcoming). https://doi. org/10.2308/HORIZONS-2020-101
46- Jasa, N. (2020). Risk disclosure and event impact mitigation: Evidence from security breaches (Doctoral dissertation of the Graduate School of the University of Colorado at Boulder for the degree of Doctor of Philosophy Department of Business Administration, Accounting 2020).
47- Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm Use of Cybersecurity Risk Disclosures. Journal of Information Systems, 36(1), 151-180.
48- Juma'h, A. H., & Alnsour, Y. (2021). How Do Investors Perceive the Materiality of Data Security Incidents. Journal of Global Information Management (JGIM), 29(6), 1-32.

49- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749.
50- Kelton, A. S., & Pennington, R. R. (2021). Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. Journal of Information Systems, 34(3), 133-157.
51- Kolesnikov, O., Markov, A., Smagulov, D., & Solovjovs, S. (2022). Cyber Loss Distribution Fitting: A General Framework towards Cyber Bonds and Their Pricing Models. International Journal of Mathematics and Mathematical Sciences, 2022.
52- Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies?. Auditing: A Journal of Practice & Theory, 37(1), 139-165.
53- Lee, Y. T. (2018). Security Breach Disclosure (Doctoral dissertation on the School of Graduate Studies, McMaster University , DeGroote School of Business.
54- Legenchuk, S. F., Vyhivska, I. M., & Grigorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security. Problems of theory and methodology of accounting, control and analysis, (2 (52)), 40-46.
55- Manoj, K. S. (2021). BANKS'HOLISTIC APPROACH TO CYBER SECURITY: TOOLS TO MITIGATE CYBER RISK. Technology, 12(1), 902-910.
56- Marinova, R. (2022). Accounting aspects of the risk of digital payment operations in Bulgarian banks. Notices of the Union of Scientists-Varna. Economic Sciences Series, 11(2), 105-113.
57- 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.
58- Masuch, K., Greve, M., Trang, S., & Kolbe, L. M. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies?. Computers & Security, 112, 102502.
59- McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 580-615.
60- Mironchuk, Z. P., & Maletska, O. I. (2022). ORGANIZATION OF ACCOUNTING PROTECTION IN CYBER SECURITY INFORMATION. Actual problems of modern business: accounting, financial and management aspects, 152-155.
61- Mitts, J., & Talley, E. (2019). Informed trading and cybersecurity breaches. Harv. Bus. L. Rev., 9, (1), 1-53.
62- Muravskyi, V., Farion, V., & Hrytsyshyn, A. (2022). QUALITY OF ACCOUNTING INFORMATION AND PRINCIPLES OF ITS CYBER PROTECTION. Scientific Notes of Ostroh Academy National University," Economics" Series, (23 (51)), 103-109.
63- Muravskyi, V., Shevchuk, O., Muravskyi, V., & Lapsinskyi, V. (2022). Improving the accounting policy of the enterprise for its cyber protection. Herald of Economics, (1), 107-124
64- Muravskyi, V., Zadorozhnyi, Z. M., Lytvynenko, V., Yurchenko, O., & Koshchynets, M. (2022). Classification of cyber risks in accounting. Herald of Economics. Independent Journal of Management & Production, 13(3), 129-167.
65- Napolitano, G. A .(2023).literature review on the role of cybersecurity in changing management accounting, auditing and governance.

66- Nie, D., & Xu, C. (2021). Non-GAAP earnings quality in firms with data breach incident. Asian Review of Accounting.
67- Obaydin, I., Xu, L., & Zurbruegg, R. (2021). The Unintended Cost of Data Breach Notification Laws: Evidence from Managerial Bad News Hoarding. Available at SSRN 3926962.
68- Orlando, A. (2021). Cyber risk quantification: Investigating the role of cyber value at risk. Risks, 9(10), 184.
69- Pacheco-Paredes, A., & Wheatley, C. M. (2022). Do Auditors Consider Cybersecurity Insurance in Pricing Audits?. Available at SSRN 4171153.
70- Peng, J., & Li, C. W. (2022). Security breaches and modifications on cybersecurity disclosures. Journal of Accounting and Management Information Systems, 21(3), 452-470.
71- Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 159, 106022.
72- Ramírez, M., Rodríguez Ariza, L., & Gómez Miranda, M. E. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability, 14(3), 1390.
73- Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. European Accounting Review, 31(3), 701-728.
74- Salvi, A., Vitolla, F., Rubino, M., Giakoumelou, A., & Raimo, N. (2021). Online information on digitalisation processes and its impact on firm value. Journal of Business Research, 124, 437-444.
75- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.
76- Sebastian, G. (2022). Could incorporating cybersecurity reporting into SOX have prevented most data breaches at US publicly traded companies? An exploratory study. International Cybersecurity Law Review, 1-17.
77- Serag, A. A., & Daoud, M. M. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. Trade and Finance, 42(1), 20-61.
78- Serkan, A. K. I. N., & Ahmet, T. A. N. C. (2022). THE IMPORTANCE OF CYBER SECURITY RISKS IN SUPERVISION OF INFORMATION SYSTEMS IN BUSINESSES. Erciyes Academy, 36(2), 707-722.
79- Shahid, S. N., & Hau Huang, E. (2020). The impact of data breaches: The organizational security measures and the individual perception of an organization's security attempts.
80- Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1), 138-156.
81- Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60.

82- Song, V., Cavusoglu, H., Lee, G. M., & Ma, L. Z. (2020). Firm actions toward data breach incidents and firm equity value: An empirical study. Proceedings of the 53rd Hawaii International Conference on System Sciences 2020,p6033- 6039.
83- Strupczewski, G. (2021). Defining Cyber Risk, Safety Science, vol. 135, 105-143 available at: https://rev4.uek.krakow.pl/wp-content/uploads/2021/03/PW2-A18.pdf
84- Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk Analysis.
85- Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. Journal of Forensic and Investigative Accounting, 12(2), 197-212.
86- Tan, H. T., & Yu, Y. (2018). Management's responsibility acceptance, locus of breach, and investors' reactions to internal control reports. The Accounting Review, 93(6), 331-355.
87- Tong, S.(2023).The Effectiveness of Information Disclosure under Cyber Attack. University of Miami Coral Gables, FL 33124 available at: https://aemps.ewapublishing.org/media/a6388e44283449d0a1953560ee2f01ba_OgnZqP9.pdf
88- Tosun, O. K. (2021). Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, 1-15.
89- Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. Information & Computer Security, 26 (5), 637-652.
90- Uddin, M., Ali, M., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.
91- Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & security, 105, 102239.
92- Vlčko, J., & Meluchová, J. (2022). Managing risks of automatic accounting. VEDECKÉ STATE A DISKUSIE, 71.
93- Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management. Vol. 28 No. 1, 167-183.
94- Zadorozhnyi, Z. M., Muravskyi, V., & Muravskyi, V. (2021, September). Combined Outsourcing of Accounting and Cybersecurity Authorities. In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 544-547). IEEE.

- **Conferences and Reports:**

1- AICPA. 2018. Communications of cybersecurity incidents: Comparison between SEC Release 33-10459 and the AICPA's Cybersecurity Risk Management Framework. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/comparison-of-sec-release-33-10459.pdf.
2- AICPA. Cybersecurity Risk Management Reporting; 2018; pp. 1–7. Available online: https://us.aicpa.org/content/dam/aicpa/

3- Akingump(www.akingump.com/en/) .(2022).Disclosing Cyber Incidents and Risks: SEC Proposes Rules to Enhance and Standardize Cyber Disclosures and Incident Reporting by Public Companies.(March 11, 2022). available at: https://www.akingump.com/a/web/bFZmDNXNuM3qu6to5VvftL/3S52xG/corporate-alert.pdf.
4- Axelrod. C. W. (2022). Reducing Cybersecurity Security Risk From and to Third Parties. .(15 June 2022). Available at: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2022/volume-3/reducing-cybersecurity-security-risk-from-and-to-third-parties__joa_eng_0622.pdf
5- BCBS. (2018). Cyber-resilience: Range of practices. Bank For International Settlements. available at: https://www.bis.org/bcbs/publ/d454.htm.
6- BIS. (2021). Cyber resilience practices - Executive Summary. available at: https://www.bis.org/fsi/fsisummaries/cyber_resilience.htm.
7- CENTRAL BANK OF BAHRAIN.(2021).Appendix RM-1 Cyber Security Incident Report. Volume 3: Insurance. Available at: https://www.cbb.gov.bh/wp-content/uploads/2021/07/Vol-4_Appendix-RM-1-Cyber-Security-Incident-Report.pdf.
8- Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17(4), 356-374.
9- Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis, August, mimeo.
10- Financial Reporting Council. (2022). FRC Lab Report: Digital Security Risk Disclosure. available at: https://www.frc.org.uk/getattachment/d54abc51-b30e-4238-8416-722bd89d9282/FRC-Digital-Security-Risk-Disclosure-Example-Bank_August-2022.pdf.
11- ICAEW Insights.(2017). CYBER-SECURITY IN CORPORATE FINANCE.(10 January 2017) . available at: https://www.icaew.com/-/media/corporate/files/technical/corporate-finance/corporate-finance-faculty/cyber-security-in-financial-services.ashx.
12- IFAC.(2019) , Cybersecurity Is Critical for all Organizations – Large and Small, Steve Ursillo, Jr., Christopher Arnold November 4.
13- IFAC.(2019) , Cybersecurity Is Critical for all Organizations – Large and Small, Steve Ursillo, Jr., Christopher Arnold November 4.
14- IFRS. (2022, 01 20). IAS 23 Borrowing Costs. Retrieved from IFRS Foundation: https://www.ifrs.org/issued-standards/list-of-standards/ias-23-borrowing-%20costs/#about
15- Information Systems Audit and Control Association (ISACA), (2017), ISACA, (2019) ,auditors have a role in cyber resilience ISACA JOURNAL VOL 6 available at www.isaca.org.
16- IOSCO/MR/17/2019. Madrid, 18 June 2019. IOSCO urges authorities to use existing standards to address cyber risk. availab at: https://www.iosco.org/news/pdf/IOSCONEWS536.pdf.
17- Luque, F. J. H., López, J. M., & Williams, P. (2021). Cyber risk as a threat to financial stability. FINANCIAL STABILITY REVIEW. Financial Stability Magazine/Bank of Spain, primavera 2021, p. 181-205.

18- Moncayo, D., & Montenegro, C. (2019, October). Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector. In 2016 6th International Conference on Information Communication and Management (ICICM) (pp. 115-120). IEEE.
19- OSFI. (2021). Technology and Cyber Security Incident Reporting. available at: https://www.osfi-bsif.gc.ca/Eng/Docs/TCSIR.pdf
20- Posner. C.(2022). Audit Analytics reports on cybersecurity disclosure.(April 11, 2022). Available at: https://cooleypubco.com/2022/04/11/audit-analytics-cybersecurity-disclosure/
21- SEC .(2022). March 9, 2022 The Securities and Exchange Commission today proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. https://www.sec.gov/news/press-release/2022-39
22- SEC. (2018). Commission statement and guidance on public company cybersecurity disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.
23- Sharma, K., & Mukhopadhyay, A. (2022). Cyber-risk assessment and mitigation of DDoS attacks using semi-structured data models.
24- The International Accounting Standards Board (IASB)IASB Agenda ref 15A .(2020). STAFF PAPER. (May 2020), 57-63. Available at: https://www.ifrs.org/content/dam/ifrs/meetings/2020/may/iasb/ap15a-management-commentary.pdf.
25- Trautman, L. J., & Newman, N. (2022). A Proposed SEC Cyber Data Disclosure Advisory Commission.
26- World Economic Forum (WEF). 2022. Cybersecurity is an Environmental, Social and Governance Issue. Available at: https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/