جامعة مدينة السادات

قسم المحاسبة والمراجعة

قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك "دراسة تطبيقية"

إعداد

الباحث/ عمرو عادل عبدالفتاح موسى
مدرس مساعد بقسم المحاسبة والمراجعة
كلية التجارة – جامعة مدينة السادات

إشراف

أ.د/ عبدالحميد أحمد أحمد شاهين
أستاذ المراجعة المتفرغ
وعميد الكلية الأسبق
كلية التجارة- جامعة مدينة السادات

أ.م.د/ محمد موسى على شحاتة
أستاذ المحاسبة المساعد
ورئيس قسم المحاسبة والمراجعة
كلية التجارة- جامعة مدينة السادات

د/ مروة أحمد عبدالرحمن البحيري
مدرس بقسم المحاسبة والمراجعة
كلية التجارة- جامعة مدينة السادات

المجلة العلمية للدراسات والبحوث المالية والإدارية
كلية التجارة - جامعة مدينة السادات
المجلد السادس عشر – العدد الرابع – ديسمبر 2024

2024 م - 1445 هـ

مستخلص البحث:

استهدف البحث تسليط الضوء على آليات الإفصاح عن المخاطر السيبرانية، واستخلاص إطار محاسبي للإفصاح عن المخاطر السيبرانية وحوكمة إدارتها، وبيان أثر تبني محاور الإفصاح عن بنود هذا المؤشر علي تكلفة رأس المال المقترض والمملوك، وذلك **كدراسة تطبيقية** في البيئة المصرية، على عينة نهائية لـ (10) بنوك، و(12) شركة بقطاع الاتصالات والاعلام وتكنولوجيا المعلومات، تكون (132) مشاهدة (شركة/سنة) خلال الفترة (2017– 2022). **وتوصلت النتائج** إلى أن شركات العينة تفصح عن المخاطر السيبرانية **بمتوسط عام بلغ (32.62)**، وبنسبة **(62%) تقريباً، ووجود علاقة ارتباط سلبية معنوية** بين الإفصاح عن المخاطر السيبرانية وبين كل من: تكلفة رأس المال المقترض، وتكلفة رأس المال المملوك ، ومتوسط التكلفة المرجحة لرأس المال، حيث أن معامل الارتباط سلبي بقيمة (-0.564)، و (-0.380)، و (-0.487)، على الترتيب ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، **وأسفرت نتائج تحليل الانحدار** عن **وجود أثر سلبي ومعنوي** للإفصاح عن المخاطر السيبرانية على كل من: تكلفة رأس المال المقترض (الديون)، وتكلفة رأس المال المملوك (حقوق الملكية)، ومتوسط التكلفة المرجحة لرأس المال، حيث أن **(R^2)** سلبي، بقيمة (0.394)، و (0.213)، (0.226)، **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 سيناريوهات 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.

الكلمات المفتاحية: الإفصاح عن المخاطر السيبرانية، تكلفة الديون، تكلفة حقوق الملكية، المتوسط المرجح لتكلفة رأس المال.

Abstract:

The research sought to shed light on the mechanisms for disclosing cyber risks, extract an accounting framework for disclosing cyber risks and the governance of their management, and demonstrate the impact of adopting the axes of disclosure of the items of this indicator on the cost of borrowed and owned capital, as an applied study in the Egyptian environment, on a final sample of (10) banks, and (12) companies in the communications, media and information technology sector, with (132) views (company/year) during the period (2017-2022) , and the results concluded that the sample companies disclose cyber risks with an overall average of (32.62) , By approximately (62%) , there is a significant negative correlation between the disclosure of cyber risks and each of: (the cost of borrowed capital (cost of debt) , the cost of owned capital (cost of equity) , and the weighted average cost of capital, as the CEfficient The correlation is negative with a value of (-0.564) , (-0.380) , and (-0.487) , respectively, and the level of significance (sig) reached (0.000) less than (0.01) . The results of the regression analysis resulted in a negative and significant effect of disclosing cyber risks. On each of: (the cost of borrowed capital (debt) , the cost of owned capital (equity) , and the weighted average cost of capital) , where (R^2) is negative, with a value of (0.394) , (0.213) , (0.226) , 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 significant cyber risks that may affect their business and financial results, and to disclose their scenario for confronting cyber risks, managing them, and mitigating their severity, in addition to issuing an accounting standard to regulate Measurement and disclosure of cyber risks, and their current and potential effects on accounting assumptions and principles and on financial statements and reports.

Keywords: Cyber Risk Disclosure, Cost of Debt, Cost of Equity, Weighted Average Cost of Capital.

أولاً: الإطار العام للبحث

1- مقدمة البحث:

أدى ظهور الأدوات الحديثة في نظم وتكنولوجيا المعلومات الرقمية إلى ترابط غير مسبوق، وأثرت على قيمة الشركة عن طريق زيادة التدفقات النقدية المتوقعة وخفض تكلفة رأس المال (Salvi et al., 2021, p 438) . وبلغت قيمة سوق الأمن السيبراني العالمي 150.37 مليار دولار أمريكي في عام 2021، ومن المتوقع أن تصل قيمته إلى 317.02 مليار دولار أمريكي بحلول عام 2027، مسجلاً معدل نمو سنوي 13.37٪ خلال الفترة المتوقعة من 2022إلى 2027(Mordor Intelligence, 2022, p1; Sonic Wall, 2022; p5).

وتقدر التكلفة السنوية العالمية للجرائم السيبرانية بـ6 تريليون دولار سنوياً ومن المتوقع أن تنمو إلى 10.5 تريليون دولار عام 2025، ولهذا السبب لا توجد طريقة للبقاء في مأمن تماماً من تهديدات الأمن السيبراني، إلا في وجود ضوابط داخلية جيدة (O'Connell, 2023, p3) . ومع تزايد التحول الرقمي والرقمنة السريعة، يتزايد التهديد السيبراني ضد المؤسسات المالية والشركات (Gulyás& Kiss,2023, p85) . وتؤثر هذه الانتهاكات في المقام الأول على القطاعات التكنولوجية والمالية بأسوأ طريقة ممكنة (Lenka et al., 2023, p172) . وتشكل المخاطر السيبرانية خطراً مستمراً ومتصاعداً على الشركات والمستثمرين والمشاركين في السوق (SEC, 2022, p6) . ولا تزال الشركات التي تجمع البيانات وتخزنها وتستخدمها، تتحمل مخاطر مالية غير معروفة من خرق محتمل للبيانات (Theriot and Gowan, 2023, p2) .

وتعتبر تكلفة رأس المال ركيزة أساسية لممارسة الأنشطة المختلفة لبقاء الشركة ونموها، كما أن الشركات المقترضة ليست متساوية في نظر المستثمرين، من حيث قدرتها على السداد والنمو (Havakhor et al., 2021, p7) . ويعتبر تقييم تكلفة رأس المال ذا أهمية حيوية لاستمرارية الشركات على المدى الطويل وقدرتها على توليد الثروة للمساهمين (Immonen, 2023, p1) . وتؤدي أدوات التكنولوجيا الحديثة إلى زيادة المخاطر السيبرانية، مما يؤدي إلى إرتفاع تكلفة رأس المال وحدوث تقلبات كبيرة في أرباح الأسهم، وبالتالي تخفيض القيمة السوقية للأسهم (Dow et al., 2017, p18) . وقد يؤدي الإفصاح عن المعلومات السلبية حول الأمن السيبراني إلى زيادة تكلفة رأس المال وكشف المعلومات السرية لكل من المنافسين والمهاجمين (الأمير، 2022، ص495؛ McGrath et al., 2022, p9) . وذلك على عكس نتائج دراسة (Elmawazini et al., 2023)، التي توصلت إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض تكلفة رأس المال. كما أن الإفصاحات المتعلقة بالأمن السيبراني للشركة ستؤدي أيضاً إلى تقليل عدم تناسق المعلومات بين إدارة الشركة ومستثمريها، وهذا يمكن أن يقلل من تكلفة رأس مال الشركة (Lenka et al., 2023, p176) .

ويركز المنظمون مثل (SECوPCAOB) اهتمامهم على كيفية معالجة ومراقبة المخاطر السيبرانية في التقارير المالية، وتقديم التقارير إلى مستخدمي البيانات المالية (Bricker et al., 2022; Hughes et al., 2023, p4) . 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 إطار عمل للتقرير عن هذه المخاطر، من خلال **ثلاث أجزاء رئيسية** من المعلومات وهي: (وصف الإدارة لبرنامج إدارة المخاطر السيبرانية للشركة، وتأكيدات الإدارة بشأن فعالية ضوابط الأمن السيبراني، ورأي المراجع بشأن إفصاحات الإدارة) (Kelton and Pennington, 2020, p.137 ; الرشيدي، عباس، 2019، ص 445) . وتتبنى حوالي 29% من الشركات في S&P 500 طواعية هذا الإطار، وهو ما يمثل 10.9 تريليون دولار من إجمالي القيمة السوقية (Schoenfeld , 2022; Frank et al., 2023, p2) .

واجتذبت الهجمات والمخاطر السيبرانية المتزايدة انتباه أصحاب المصلحة والممارسين وهيئات الحوكمة، الذين دعوا مجالس الإدارة للقيام بدور أكثر نشاطاً في توفير إشراف شامل على هذه المخاطر السيبرانية وضرورة المشاركة في مراقبة المخاطر السيبرانية (Hartmann and Carmenate, 2021, p.14) . وحتى في غياب قوانين ولوائح واضحة للأمن السيبراني، ومع زيادة وعي أصحاب المصلحة بالمخاطر السيبرانية، تميل الشركات إلى الإفصاح الإختياري عن المعلومات المتعلقة بالمخاطر السيبرانية (Yang et al., 2020, p178) . وذلك لمحاولة للتخفيف من أي مخاطر محتملة أو مخاطر حدثت من خلال زيادة الشفافية التي ستبني ثقة جميع أصحاب المصلحة (Lenka et al., 2023, p169) . ونظراً لتزايد أحداث الأمن السيبراني التي لها عواقب اقتصادية سلبية على الشركات وأصحاب المصلحة، يتوقع المستثمرون المزيد من المعلومات حول تعرضات الأمن السيبراني للشركة، ونظراً لعدم تناسق المعلومات بين الشركات وأصحاب المصلحة، يتعين على المستثمرين عموماً الاعتماد

على التقارير العامة للشركات حول مخاطر الأمن السيبراني، ومع ذلك، لا يوجد سوى إفصاح محدود متاح حول قضايا الأمن السيبراني للشركات نظراً لعدم وجود متطلبات قانونية صريحة لمثل هذا الإفصاح (Cheong et al., 2021; Shaker et al., 2023; Saleh, 2023, p59) . وإن أي حادث سيبراني يتعلق بشكل مباشر بالنظام المحاسبي للشركة قد يؤثر على بياناتها المالية، وحتى الخروقات التي لا تؤثر بشكل مباشر على النظام المحاسبي، قد تشير إلى ضعف في الضوابط الداخلية، مما يشير إلى مخاطر بالنسبة للرقابة الداخلية على التقارير المالية (Huang et al., 2024, p13).

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 المخاطر السيبرانية 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). **وكنتيجة حتمية لما سبق**، تقوم الشركات 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 (Berkman et al., 2018, p.509-510) . وبالنظر في أدبيات الفكر المحاسبي، يتضح أن المخاطر السيبرانية يمكن أن يكون لها تكاليف اقتصادية سلبية تؤثر على عمليات وأنشطة الشركة، وقرارات إعداد التقارير المالية، والإفصاحات، وتصورات أصحاب المصلحة الخارجيين (Li and Walton, 2023, p2,3) . واتجهت التحديثات الأخيرة نحو الإفصاح عن المخاطر السيبرانية، سواء كانت كمية أو نوعية، في تقارير البنوك والشركات (Shehata et al., 2023, p4, 5) .

وفي ضوء ما سبق، يسعي البحث إلى تسليط الضوء على آليات الإفصاح عن المخاطر السيبرانية، واستخلاص مؤشر محاسبي لآليات الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها، وذلك بالارتكاز على التوجيهات والإرشادات المحاسبية الصادرة من قبل الجهات المهنية والتنظيمية، ودراسة وتحليل الآثار الجوهرية لهذه الإفصاحات على القوائم المالية والتقارير السنوية والإفصاحات ذات الصلة، وقياس أثر تبني محاور الإفصاح عن بنود هذا المؤشر على تكلفة رأس المال المقترض والمملوك، وبما يتلاءم مع بيئة الأعمال المصرية في ضوء التحول الرقمي والحوكمة السيبرانية والرقمنة، فضلاً عن تقديم دراسة تطبيقية.

2- مشكلة 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) .

وتحظى تكلفة رأس المال بأهمية كبيرة في الفكر المحاسبي، حيث يعد من أهم محددات نجاح الشركة واستمراريتها، كما اهتم الفكر المحاسبي بقيمة المنشأة، خاصةً بعد تحول هدف المنشأة من العمل على تعظيم ربحيتها إلى العمل على تعظيم قيمتها. وتوصلت دراسة (Sumardani and Handayani, 2019) الى أن مستوى الإفصاح عن مخاطر الشركات له تأثير سلبى على تكلفة رأس المال، وأن حجم المعلومات الذي تفصح عنه الشركة سيقلل من تكلفة رأس المال، ولها تأثير إيجابي على قيمة المنشأة. وتوصلت دراسة (Havakhor et al., 2021) أن الإفصاح عن معلومات الأمن السيبراني تقلل من تكلفة رأس المال عن طريق تقليل عدم تناسق المعلومات حول قدرة الشركة على التعامل مع المخاطر السيبرانية. وأصبح التعامل في الفضاء السيبراني أحد المخاطر الرئيسية التي يجب أن تتعامل معها الشركات، حيث أصبحت المخاطر السيبرانية أحد أكبر أشكال المخاطر على المستوى الدولي، مما يضر بأنظمة تكنولوجيا المعلومات بالشركات في جميع أنحاء العالم (Savaş and Karataş, 2022, p14; Poddar, 2023, p5; Pollmeier et al., 2023, p1) .

وبالنسبة للأوضاع في البيئة المصرية، فإن **61%** من المنشآت المصرية ليس بها حماية كافية للمعلومات، وبلغت خسارتها المالية نحو**3.78**مليون دولار (المركز المصري للدراسات الاقتصادية، 2019) . 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 220٪. ووفقاً للتقرير السنوى الصادرعن المركز الوطني للاستعداد لطوارئ الحاسبات والشبكاتEG-CERT لعام 2019/2018 أن أكثر القطاعات تعرضاً للحوادث السيبرانية في مصر هو قطاع الاتصالات وتكنولوجيا المعلومات بنسبة 42٪ 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 57.6%. وقد تعرضت مصر للعديد من هذه الهجمات فوفقاً للتقرير الصادر عن شركة" تريند مايكرو" عام 2018، فإن إجمالي عدد البرمجيات الخبيثة التي إكتشفتها Kaspersky في البلاد قد وصل إلى 242,411 برمجية خبيثة خلال الربع الأخير من عام 2017 وحده ما يمثل زيادة بنسبة 25%عن الربع الثالث من نفس العام والذي شهد اكتشاف 194,719 برمجية خبيثة (المركز العربي للبحوث والدراسات، 2020) . وبحسب المؤشر العالمي للأمن السيبراني (GCI)، والمكون من 46 مؤشر مختلف، والذي يصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة، فإن مصر تقع في المرتبة الـ 14عالمياً والثالثة عربياً عام 2017، وتقع في المرتبة الـ 23عالمياً والرابعة عربياً عام 2019، وعلى الرغم من أن مصر تقع في تصنيف الدول الأعلى التزاماً بالأمن السيبراني محققة (0.842) درجة، إلا أنها تراجعت في الترتيب العالمي (9) مراكز وعربياً مركزاً واحداً (GCI, 2020, p57) .

وتعرضت مصر إلى **310,000 هجمة خبيثة** خلال الفترة من يناير إلى مايو 2021، وتحتل المرتبة الخامسة في عدد الهجمات الاحتيالية الخبيثة، وفي الربع الأول من عام 2021، واجهت مصر أعلى معدلات الاكتشاف في جميع أنحاء إفريقيا، وتمثل وحدها ما يقرب من 35٪ من إجمالي اكتشافات برامج الفدية الضارة في إفريقيا (Interpol, 2021, p8, 15, 23) . وتشكل التهديدات السيبرانية مصدر متزايد إفريقيا، حيث تعمل90٪ من الشركات الأفريقية بدون وجود ضوابط الأمن السيبراني اللازمة (Sarefo et al., 2023, p1013) .

وتتجسد مشكلة البحث في أنه لا يوجد شروط وضوابط محددة للإفصاح عن المخاطر السيبرانية في التقارير السنوية، وعدم توافر إطار محدد لتوجيه الشركات للإفصاح والتقرير عنها، وحوكمة إدارتها، وعدم وجود قواعد متعددة الأطراف تحكم التخفيف من هذه المخاطر، ولم يتم تقديم أي دليل تطبيقي حول كيفية قياس المخاطر السيبرانية من الناحية الكمية، وكذلك لم تصدر الهيئة العامة للرقابة المالية أو البورصة المصرية أو البنك المركزي؛ أية تعليمات لتوجيه الشركات للإفصاح عن ممارسات الأمن السيبراني والمخاطر التي تتعرض لها وحوكمة إدارتها، وعدم وجود أدلة تطبيقية في البيئة المصرية لقياس أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها على مؤشرات قياس تكلفة رأس المال (المقترض والمملوك)، مما دعى إلى محاولة بناء مؤشر محاسبي مقترح للإفصاح عن المخاطر السيبرانية وحوكمة إدارتها على مؤشرات قياس تكلفة رأس المال رأس المال المقترض والمملوك، وذلك كدراسة تطبيقية بالبيئة المصرية.

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

1- ما مدى كفاية محتوى الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها في القطاعات المصرية محل الدراسة (البنوك- تكنولوجيا المعلومات والاتصالات والإعلام) ؟
2- ماهي طبيعة واتجاه العلاقة بين الإفصاح عن المخاطر السيبرانية ومؤشرات قياس تكلفة رأس المال المقترض والمملوك؟
3- ما هو أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك؟

3- 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:

1/3- دراسات اهتمت بالإفصاح عن المخاطر السيبرانية:

استهدفت دراسة (Duvenhage et al., 2022) على تحليل ومقارنة ممارسات الإفصاح 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 2018. **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 (48 كلمة) متعلقة بالأمن السيبراني أكبرمن عدد الكلمات في البنوك الصينية (7كلمات)، ولم يتم الإفصاح عن حادثة واحدة تتعلق بالمخاطر السيبرانية للسنة المالية 2018. 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 2006إلى 2018، وباستخدام عينة من 558 ملاحظة/سنة للشركات الربحية (التجارية)، تمثل 279 سنة - المنشآت مقسمة إلى (279سنة/ شركة مخترقة) و (279سنة/ شركة غير مخترقة) بإجمالي (1.116) 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، 2022)** 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 2019-2020. **وتوصلت** 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. **واستهدفت 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 20 نموذجاً سنوياً للشركات ذات أعلى قيمة سوقية في الأوراق المالية في دول الأرجنتين والبرازيل وشيلي وكولومبيا والمكسيك وبيرو خلال الفترة (2016-2020) في **أربع قطاعات** (الطاقة، المالي- القطاع التقديري للمستهلكين- المواد) . وأن أعلى نسبة إفصاح ذات صلة هي الأرجنتين، ويرجع الفضل في الإفصاحات الأكثر شمولاً إلى القطاع المالي؛ ويمثل بُعد الاستراتيجية أكبر وزن في درجة المؤشر.

وقامت دراسة **(Firoozi and Mohsni, 2023)** بالتحقيق في إفصاحات الأمن السيبراني التي قام بها أكبر 48 بنكاً كندياً وأمريكياً في الفترة من 2014 إلى 2020، حيث أن القطاع المصرفي هدفاً رئيسياً للهجمات السيبرانية بسبب البيانات الهامة التي يحتوي عليها، وذلك باستخدام منهج نوعي استكشافي، وقامت الدراسة أولاً بتطوير مؤشر بناءً على الأدبيات السابقة والسياسات الحالية بشأن الافصاح عن الأمن السيبراني والتشاور مع الأكاديميين والممارسين، ثم استخدمت المؤشر لترميز تقارير البنوك المتعلقة بالأمن السيبراني يدوياً، وتم التحقق من محتوى الإفصاحات بالتفصيل ومناقشة مستوى الالتزام بالمؤشر، ثم حللت بشكل نقدي سلوكيات الإفصاح لدى البنوك باستخدام نظرية تكلفة الملكية ونظريات الإشارة والشرعية. **وأظهرت النتائج** أنه بينما كان هناك تحسن في الافصاح عن الأمن السيبراني في القطاع المصرفي، فإن الإفصاحات منخفضة نسبياً في المجالات الحيوية للحوكمة والمخاطر وتخفيف المخاطر، بالإضافة إلى ذلك، توصلت الدراسة إلى أن البنوك الأمريكية لديها مستويات أعلى بكثير من الإفصاح من الناحيتين النوعية والكمية من البنوك الكندية. وفحصت دراسة **(Ereddia, 2023)** العوامل المرتبطة بشفافية الشركة في رقابة مجلس الإدارة للمخاطر السيبرانية، حيث تتطلب لجنة الأوراق المالية والبورصات، إلى الحد الذي تكون فيه المخاطر السيبرانية جوهرية، أن تكشف الشركات عن طبيعة دور مجلس الإدارة في الإشراف على إدارة تلك المخاطر، باستخدام التحليل النصي، حددت 2921 شركة أبلغت عن عوامل

مخاطر جوهرية للأمن السيبراني في تقاريرها السنوية، من خلال تقاريرها لعام 2021 الخاصة بهذه الشركات، وجمعت البيانات المتعلقة بـ 12 عنصراً مختلفاً من عناصر إشراف مجلس الأمن السيبراني، وانشاء درجة شفافية شاملة (T- Score)، **ووجدت الدراسة** أن أكثر من 36%من الشركات لا تقدم أي معلومات حول دور مجلس الإدارة في الإشراف على المخاطر السيبرانية، على الرغم من أن هذه الشركات تكشف عن مخاطر سيبرانية جوهرية في افصاحات (SEC)، وفي التحليل متعدد المتغيرات، وجدت أن مستوى الإفصاح المتعلق برقابة مجلس الإدارة مرتبط بشكل إيجابي بمستويات المخاطر السيبرانية وحجم الشركة.

وفي هذا السياق، **حاولت دراسة (Jin et al., 2023)** استكشاف محددات الهجمات السيبرانية على البنوك التجارية، وتأثيرها على سلوك إدارة الأرباح لتلك البنوك، وبحثت في إمكانية وكيفية توقع هجوم سيبراني على أحد البنوك باستخدام مقاييس المحاسبة المالية، وتناولت هذه الدراسة قياس تأثير أحكام خسائر القروض التقديرية كمؤشر لضعف الرقابة الداخلية في البنوك على الهجمات السيبرانية، وما إذا كانت البنوك تقوم بإدارة أرباح أقل أو أكثر بعد الهجوم السيبراني، وتكونت العينة النهائية من (44.347) مشاهدة خلال الفترة 2004-2019. **وتوصلت** الدراسة إلى أن البنوك التي لديها المزيد من مخصصات خسائر القروض التقديرية تواجه المزيد من الهجمات السيبرانية؛ أي أن مخصصات خسارة القروض التقديرية مرتبطة بشكل إيجابي بالهجمات السيبرانية المستقبلية، بينما تشارك البنوك في إدارة أرباح أقل لتجنب الخسارة في أعقاب مثل هذه الهجمات؛ أي أن البنوك ستشارك في إدارة أرباح أقل بعد مثل هذه الحوادث، وذلك ربما بسبب تحسين الرقابة الداخلية. **وأخيراً، سلطت دراسة (Huang et al., 2024)** الضوء على قياس التأثير السلبي لتأخير الإفصاح عن الهجمات السيبرانية، وتوضيح كيفية تأثير التأخير في الإفصاح عن الهجمات السيبرانية على الأداء المالي وعواقبها المحتملة على ربحية الشركات، وذلك باستخدام عينة نهائية من 278 شركة أمريكية، مكونة من 326 مشاهدة/ حالة هجوم سيبراني خلال الفترة من 2005 إلى 2021. **وتوصلت نتائج الدراسة** إلى أن التأخير في الإفصاح عن الهجمات السيبرانية يرتبط عكسياً بربحية الشركة، ويعزو ذلك إلى عدم تناسق المعلومات، حيث أن انخفاض إمكانية قراءة التقارير المالية يمكن أن يفسر التأثير السلبي للتأخير في الإفصاح، وأن هذا التأثير السلبي يتم تخفيفه من خلال وجود رئيس قسم المعلومات، وأكدت النتائج على ضرورة قيام المنشآت بإعطاء الأولوية لعمليات الافصاح عن المخاطر السيبرانية في الوقت المناسب وبشكل شفاف، وتنفيذ آليات قوية للاستجابة للحوادث.

2/3- دراسات تناولت العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال:

قامت **دراسة (Havakhor et al., 2021)** بتحليل المسار المحتمل لخلق القيمة من خلال استثمارات الأمن السيبراني وتخفيض تكلفة رأس مال والإفصاح عنها، وتحليل رد فعل سوق رأس المال، وتم **تطبيق الدراسة** على 74.755 ملاحظة لـ 6.058 شركة نشطة خلال الفترة من عام 2000 إلى عام 2018، وتم إستخدام أسلوب تحليل المحتوى. **ووجدت الدراسة** أن الإفصاح عن استثمارات الأمن السيبراني ترتبط بالإنخفاض في تكلفة رأس المال، وترتبط إيجابياً بشكل عام على تعزيز القيمة للمنشأة، كما أن الإفصاح عن معلومات الأمن السيبراني ومدى تغطية المحللين للشركة يعزز الاستثمار في الأمن السيبراني وتكلفة رأس المال، وأن معاملات مؤشر الإفصاح عن المخاطر السيبرانية DCRs، جميعها غير دالة إحصائياً على تكلفة رأس المال، وبالتالي مجرد الإفصاح عن المخاطر السيبرانية دون شرح الإجراءات الملموسة لمكافحة وتخفيف هذه المخاطر السيبرانية لا يترجم إلى تخفيض تكلفة رأس المال، وتشير نتائج نموذج الإنحدار بأن الشركة التي تقوم بالإفصاح عن الإستثمار في الأمن السيبراني تتمتع بتخفيض بنسبة 10٪ تقريباً في تكلفة معدل رأس المال في السنة اللاحقة، ويُظهر النموذج أنه يوجد تأثير جوهري وإيجابي من قبل DCIs على Tobin's Q.

في حين، استكشفت دراسة (Sheneman, 2022) في ما إذا كانت أحداث الأمن السيبراني للشركات النظيرة في صناعة ما تؤثر على تكلفة الديون الخاصة، إذا قام المقرضون بتعديل التوقعات بشأن المخاطر السيبرانية على مستوى الصناعة. وقدمت **النتائج** دليلاً على التأثيرات التنافسية وتكون أكثر وضوحاً للقروض قصيرة الأجل وغير المحددة الأجل وللصناعات ذات النمو المرتفع والرافعة المالية المنخفضة، وبشكل جماعي تشير الأدلة إلى أن الهجمات السيبرانية توفر معلومات خاصة بالشركة للمقرضين. **وحللت دراسة (Elmawazini et al., 2023)** كيفية تأثير متطلبات الإفصاح عن المخاطر السيبرانية على تكلفة رأس مال الشركة كمقياس لمخاطر المساهمين، والتي تم قياسها من خلاله، وذلك بإستخدام المرور المتدرج لقوانين الإفصاح عن خرق البيانات في الولايات المتحدة الأمريكية، وكيف يمكن أن يؤثر حجم الشركة على طبيعة العلاقة بين قوانين الإفصاح عن المخاطر السيبرانية وتكلفة رأس مال الأسهم، وذلك من خلال استخدام مجموعة كبيرة من الشركات العامة الأمريكية المدرجة في قواعد

بيانات (Compustat)، ونتج عن إجراء اختيار العينات هذا مجموعة بيانات نهائية مكونة من (36.326) مشاهدة (سنة/ الشركة) خلال الفترة من (2000-2019) . **وأظهرت نتائج الدراسة** أن إقرار قوانين الإفصاح الإلزامي عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال وذو دلالة احصائية عند مستوي معنوية (1%)، وأشارت النتائج إلى أن التأثير السلبي للإفصاح عن المخاطر السيبرانية على تكلفة رأس مال الأسهم يكون أكثر وضوحاً بالنسبة للشركات الأصغر، وأن المساهمين ينظرون إلى قوانين الإفصاح عن المخاطر السيبرانية كعامل لتقليل المخاطر.

وفي هذا السياق، قامت دراسة (Harris et al., 2023) بتحليل العلاقة بين الافصاح عن المخاطر السيبرانية وتكلفة الديون، والتحقق من خصائص تأثير الإفصاح عن المخاطر السيبرانية على تكلفة الديون، من خلال التركيز على الخصائص المميزة للإفصاح عن الأمن السيبراني، وتم قياس جودة الافصاح عن المخاطر السيبرانية من خلال ما يلي: ((1) إجمالي عدد الكلمات التي تصف المخاطر السيبرانية في إفصاحات المنشأة ؛ (2) مستوى سهولة قراءة الافصاح؛ و (3) عدد الكلمات المثيرة للجدل مقسوماً على إجمالي عدد الكلمات في إفصاحات الأمن السيبراني) على معدل العائد المطلوب للدائنين، وذلك من خلال تحليل البيانات لحجم العينة النهائية لـ421 منشأة أمريكية من عام 2007 إلى عام 2018، واستخدمت الدراسة طريقة معممة لتحليل الانحدار الديناميكي للوحة (GMM) لاختبار النماذج. **ولقد توصلت نتائج الدراسة** إلى أنه مع انخفاض جودة الإفصاح عن المخاطر السيبرانية في تقارير (10-K)، تزداد تكلفة الديون بهذه المنشآت، وأنه عندما يواجه المقرضون إفصاحات منخفضة الجودة عن المخاطر السيبرانية، فإنهم يميلون إلى اعتباره مخاطرة أعلى أو احتمال أعلى لحوادث الأمن السيبراني المستقبلية، وبالتالي فإن تكلفة الديون ترتفع، كما يتجنب المستثمرون الاستثمار في مثل هذه المنشآت الضعيفة، وأن المنشآت ذات جودة الإفصاح المنخفضة عن المخاطر السيبرانية تواجه تكلفة ديون أعلى قد تؤثر على ربحيتها الإجمالية واستدامتها على المدى الطويل، وأوصت الدراسة بضرورة تحسين جودة الافصاح لديها وأن تكون أكثر شفافية عندما يتعلق الأمر بالمخاطر السيبرانية، حيث أن تحسين جودة الإفصاح يقلل من تكلفة ممارسة الأعمال التجارية.

وأخيراً، بحثت دراسة (Chatterjee et al., 2024) في تأثير أنظمة الإفصاح الإلزامي عن المخاطر السيبرانية على مستوى الدولة (قوانين الإخطار بخرق البيانات Data Breach Notification ((DBN)) على تكلفة الديون، وذلك من خلال تسليط الضوء على تكاليف الإفصاح للشركات، والفوائد المرتبطة بهذه اللوائح، وباستخدام الإقرار المتدرج لقوانين (DBN)، وتكونت العينة الأساسية من 32,554 قرضًا تم إصدارها إلى 6,108 شركة في أنحاء الولايات المتحدة الأمريكية، خلال الفترة من 1994 إلى 2019. **وتوصلت الدراسة إلى عدد من النتائج، أهمها؛** زيادة في تكلفة الديون للشركات المتضررة من هذه القوانين، وأن قوانين (DBN) تزيد من توقعات المقرضين لمخاطر التدفق النقدي الناجمة عن التكاليف المستقبلية المحتملة المتعلقة بالإفصاح عن المخاطر السيبرانية، كما وثقت النتائج أيضًا أن الزيادة في تكلفة الديون تكون أكثر وضوحًا بالنسبة للشركات التي (1) تنتمي إلى الصناعات المعرضة لانتهاكات البيانات، أو (2) تبلغ عن نقاط ضعف في الضوابط الداخلية، أو (3) تفصح عن المخاطر السيبرانية في عامل الخطر الخاص بها، بالإضافة إلى ذلك، توصلت الدراسة إلى أن الزيادة في تكلفة الديون يتم تخفيفها في الشركات التي تركز على تدابير الأمن السيبراني، مثل الاستثمار في الأمن السيبراني أو تعيين مسؤول تكنولوجي في مجلس إدارتها.

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

- **بالنسبة للمجموعة الأولى (الإفصاح عن المخاطر السيبرانية) :** فقد أكدت على أهمية الإفصاح 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، 2022)** إلى وجود علاقة معنوية موجبة بين مستوى الإفصاح و قيمة الشركة. وأوصت دراسة **(يعقوب وآخرون،2022)** بضرورة تبني المؤشر المقترح للإفصاح عن المخاطر السيبرانية، وتوصلت دراسة **(شرف، 2023)** إلى وجود تأثير معنوي لإفصاح الشركات عن تقرير إدارة المخاطر السيبرانية علي قرارات المستثمرين المصريين غير المحترفين. وتوصلت دراسة **(Saleh, 2023)** إلى أن تقرير التوكيد المهني المستقل عن إدارة المخاطر السيبرانية (CSRM) يؤثر بشكل إيجابي على أحكام المستثمرين المصريين غير المحترفين بشأن

مدى جاذبية الاستثمار في الشركة محل الدراسة والتي تستخدم خدمات الحوسبة السحابية. **وأخيراً، أكدت نتائج دراسة (Huang et al., 2024)** على ضرورة قيام المنشآت بإعطاء الأولوية لعمليات الافصاح عن المخاطر السيبرانية في الوقت المناسب وبشكل شفاف، وتنفيذ آليات قوية للاستجابة للحوادث.

- **بالنسبة للمجموعة الثانية: (اهتمت بتناول العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال) :** وجود تباين في نتائج الدراسات السابقة؛ فقد توصلت بعض الدراسات إلى أن الإفصاح عن الأمن السيبراني يؤدي إلى زيادة وعي المستثمر وبالتالي تخفيض تكلفة رأس المال **(Song et al., 2020; Godoy, 2021)**، وتوصلت دراسة **(الفقي،2021)** إلى وجود علاقة عكسية معنوية بين هيكل رأس المال ومستوى إدارة المخاطر الرقمية، وتوصلت دراسة **(Kamiya et al., 2021)** إلى أنه عندما يترتب علي الهجوم السيبراني فقدان المعلومات المالية، يكون هناك خسارة في ثروة المساهمين بنسبة (-1.09٪)، ووجدت دراسة **(Havakhor et al ., 2021)** أن الإفصاح عن استثمارات الأمن السيبراني ترتبط بالإنخفاض في تكلفة رأس المال، وقدمت دراسة **(Sheneman, 2022)** دليلاً على التأثيرات التنافسية لأحداث الأمن السيبراني، وأكثر وضوحاً للقروض قصيرة الأجل وغير المحددة الأجل. **وأخيراً، توصلت دراستي كل من (Harris et al., 2023; Chatterjee et al., 2024)** إلى أنه مع انخفاض جودة الإفصاح عن المخاطر السيبرانية في تقارير (10-K)، تزداد تكلفة الديون بهذه الشركات.
- **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 استخلاص 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 وانعكاساتها على تكلفة رأس المال المقترض والمملوك.

4- أهداف البحث: يتمثل الهدف الرئيس 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 تكلفة رأس المال المقترض والمملوك.**وينبثق من الهدف الرئيس مجموعة الأهداف الفرعية التالية:**

1- تقييم مدى كفاية محتوى الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها وكيفية معالجتها في القطاعات المصرية محل الدراسة (البنوك- تكنولوجيا المعلومات والاتصالات) .
2- تحديد طبيعة واتجاه العلاقة بين الإفصاح عن المخاطر السيبرانية ومؤشرات تكلفة رأس المال المقترض والمملوك.
3- قياس أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها على مؤشرات تكلفة رأس المال المقترض والمملوك في القطاعات المصرية محل الدراسة (البنوك- تكنولوجيا المعلومات والاتصالات) .

5- أهمية البحث: تتمثل أهمية البحث فيما يلي:

1/5- الأهمية العلمية: تتمثل الأهمية العلمية للبحث فيما يلي:

- 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.
- 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 تعزيز ممارسات الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها.
- يتطرق البحث إلي متغيرات حديثة في الجانب النظري والعملي والتحليلي، وبذلك يشكل البحث منطلقاً جديداً لمزيد من الدراسات اللاحقة حول هذا الموضوع.

2/5- الأهمية العملية: تتمثل الأهمية العملية للبحث فيما يلي:

- تزايد أهمية الأمن السيبراني ومخاطره وتأثيراته الاقتصادية على أعمال المنشآت وأصولها، بسب التعرض للتهديدات والحوادث السيبرانية، والتي أفقدت المنشآت أموال طائلة وأثرت على أدائها، وسمعتها.
- إرساء الضوابط والأطر المنهجية في مجال الأمن السيبراني في ضوء سعي المنشآت بشكل مستمر إلى مراقبة تقارير الإفصاح لتجنب المخاطر السيبرانية.
- 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.

6- **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:

1/6- يوجد تفاوت في الإفصاح عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.

2/6- يوجد ارتباط معنوي بين الإفصاح عن المخاطر السيبرانية ومؤشرات تكلفة رأس المال المقترض والمملوك.

3/6- يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على مؤشرات تكلفة رأس المال المقترض والمملوك.

7- **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 عن المخاطر السيبرانية وإدارتها، وكيفية معالجتها والتخفيف من حدتها، **والمنهج الاستقرائى**، واعتمد 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 تكلفة رأس المال المقترض والمملوك..

8- **حدود البحث:** اقتصرت 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 6 سنوات تبدأ من عام 2017 وتنتهي بعام 2022.
- **حدود منهجية:** دراسة الجوانب المحاسبية، والتي وردت في الفكر المحاسبي، وعدم التطرق للجوانب التقنية والبرمجية لتأمين البيانات، والحد من هجمات المخاطر السيبرانية.

9- **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: دراسة تحليلية لمتطلبات الإفصاح عن المخاطر السيبرانية وإدارتها في ضوء الأطر والإرشادات التنظيمية.**
- **ثالثاً: تحليل المعايير والأطر المحاسبية والتنظيمية للإفصاح عن المخاطر السيبرانية وإدارتها.**
- **رابعاً: تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال**
- **خامساً: الدراسة التطبيقية واختبارات الفروض.**
- **سادساً: النتائج والتوصيات والدراسات المستقبلية.**

وفيما يلي عرض تفصيلي لباقي محاور خطة البحث.

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

1- طبيعة وأهمية الافصاح والتقرير عن المخاطر السيبرانية.

الإفصاح عن المخاطر السيبرانية؛ هو مجموعة 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 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، 2022، ص48-49) .

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 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.

2- الجوانب الأساسية لمتطلبات الإفصاح 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) .

1/2- عناصر الإفصاح 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(Badawy, 2021, p9). وتتمثل العناصر الأساسية المحيطة بالانتهاكات والمخاطر السيبرانية فيما يلي:-

1/1/2- الإفصاح 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 (NIST 800-53, 2019) . ويمكن للأصول المتعلقة بالمخاطر السيبرانية أن تمثل نقاط ضعف، وتتجسد المخاطر السيبرانية في استغلال نقاط الضعف هذه (Luque et al., 2021, p187). والإفصاح المنسق عن **نقاط الضعف والثغرات الأمنية (CVD)** هو مهمة جديدة تهدف إلى معالجة المرونة السيبرانية لمنتجات وخدمات تكنولوجيا المعلومات والاتصالات بشكل شامل، نظراً لأي ثغرة أمنية، يجب تضمينها في قاعدة البيانات، بالتعامل معها ومعالجتها بسرعة بمجرد الإبلاغ عنها(Giannakoulias, 2023, p41; Schmitz-Berndt, 2023, p346) .

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.

2/1/2- الإفصاح 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) .

3/1/2- الإفصاح 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(Lee, 2018, p83-84) .

4/1/2- الإفصاح 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، وفعالية الاستراتيجية، 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) .

ويرى الباحث، أنه من الضروري التحقق من جودة الإفصاح عن المخاطر السيبرانية، وأن يتضمن الإفصاح 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) .

2/2- الإفصاح الداخلي والخارجي عن المخاطر السيبرانية

1/2/2- الإفصاح 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 72 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) .

2/2/2- الإفصاح 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) .

3- الإفصاح عن حوكمة الأمن السيبراني وإدارة مخاطره

1/3- ماهية والدور المحاسبي في إدارة المخاطر السيبرانية.

أصبحت المخاطر السيبرانية والافصاح عنها أولوية قصوى لمجلس الإدارة في كل شركة، ويجبر انتشار انتهاكات البيانات الشركات على الاستثمار بكثافة في إدارة المخاطر السيبرانية وإعداد التقارير، و تتعرض الشركات لضغوط لإثبات أن لديها عمليات وضوابط فعالة لإدارة واكتشاف التهديدات السيبرانية والتعافي منها (AKÇAKANAT et al., 2021, p248) . ولذلك فإن فهم المخاطر السيبرانية وتقييمها ومراقبتها والاستجابة لها أصبح موضوعاً بحثياً مهماً في المجال المحاسبي (Janvrin and Wang, 2021, p6) .

وتشير **إدارة المخاطر السيبرانية** إلى تحديد المتطلبات (قيم الأصول، التهديدات، نقاط الضعف)، وتحليل السيناريوهات وقياس المخاطر؛ واختيار التأكيدات وتنفيذها(Maritz, 2021, p2) . وعرفتها دراسة (الصيرفي، 2022، ص4) بأنها مجموعة السياسات والاجراءات الرقابية لحماية المعلومات والأنظمة من الحوادث السيبرانية. وأشار تقرير (ISCA,2018) إلي أن تقييم المخاطر السيبرانية لا يقل أهمية عن تقييم المخاطر الأخرى، ويترتب عليها خسائر مالية وغير مالية، والتي تنعكس على بيانات التقارير المالية. ونتيجة لأهمية إدارة المخاطر السيبرانية تم تطوير إطار (COSO, 2017) تمهيداً لاستخدامه لإدارة المخاطر السيبرانية. وإن **استراتيجية التخفيف من المخاطر السيبرانية** هي خطة عمل تضعها المنظمات بعد إجراء تقييم شامل للتهديدات السيبرانية المحتملة، لتقليل الآثار السلبية أو منعها بشكل مثالي قبل حدوث أي ضرر نتيجة التعرض للهجوم السيبراني (Duvenhage et al., 2022,p 8) .

2/3- حوكمة الأمن السيبراني ومسؤولية مجلس الإدارة في مراقبة المخاطر السيبرانية

قد اكتسبت قضايا المحاسبة المتعلقة بحوكمة الأمن السيبراني وإدارته اهتماماً من واضعي معايير المحاسبة والجمعيات المهنية، وفي عام 2023، تلوح هذه التحديات في الأفق: (الإفصاحات الإلزامية، واختبارات المرونة، والضغط للحصول على أمان البيانات والخصوصية)، ويرى المديرون الحاجة إلى المضي قدماً في خمس قدرات إلكترونية هي التحديد و الإفصاح والحماية والاستجابة والتعافي (PwC, 2022) . وبالنسبة للكيانات التي يمكن أن تتأثر عملياتها بشكل كبير، من المهم للإدارة و المكلفون بالحوكمة النظر في المخاطر المتعلقة بالأمن السيبراني، ومتى قد يقع حدث الأمن السيبراني، سواء كان ذلك جوهرياً من الناحية الكمية أو النوعية والآثار المترتبة على التقرير المالي (AUASB, 2021, p5) .

ويشمل **هيكل حوكمة إدارة المخاطر السيبرانية** عملية إنشاء وصيانة والتقريرعن برنامج إدارة المخاطر السيبرانية، وإشراف مجلس الإدارة (AICPA, 2017) . ويتعلق قياس حوكمة الأمن السيبراني بالضوابط الأمنية وفعاليتها، وتتكون الضوابط من معايير السياسة العامة المادية والمنطقية الموضوعة داخل النظم والشبكات لضمان حماية المعلومات (Hess, 2021, p32; Shaker et al., 2023, p7) . وتساهم الإفصاحات المتعلقة بحوكمة الأمن السيبراني وإدارة المخاطر في زيادة ثقة أصحاب المصلحة، من خلال توضيح كيفية تنفيذ مجالس الإدارة لالتزاماتها المتعلقة بمراقبة المخاطر السيبرانية في البيئة الديناميكية، حيث يتطلب اكتساب ثقة المستثمرين حوكمة قوية للأمن السيبراني والافصاح عنها (Lenka et al., 2023, p176) .

ويري الباحث أن الحوكمة السيبرانية هي مجموعة من القواعد والإجراءات الوقائية والتصحيحية التي تحقق الرقابة على المخاطر السيبرانية، ومواجهتها وادارتها والتخفيف من آثارها المحتملة، لتحقيق المرونة والقدرة السيبرانية في تحمل التهديدات والحوادث السيبرانية المحتملة، والتعافي منها في الوقت المناسب، ولضمان استمرارية أعمال الكيان.

وأشارت دراسة (Wanlass, 2021, p1)، إلى أنه بمراجعة إفصاحات (10-K) في شركات (S&P 1500) لآخر سنة مالية اعتباراً من 31 يناير 2021. وتشمل ما يلي: (يتم تنظيم المخاطر المتعلقة بالإنترنت في الغالب من قبل لجنة محددة تابعة لمجلس الإدارة، وغالباً ما تكون لجنة المراجعة، وتفصح غالبية الشركات عن إجراءاتها الوقائية لتقليل المخاطر المتعلقة بالإنترنت. ويلعب مجلس الإدارة دوراً حاسماً في كونه الرابط الأكثر حيوية للأمن

السيبراني، حيث تعتمد القيمة الأساسية للشركة على مدى نجاحها في تأمين بياناتها، وتعزيز برامج الدفاع السيبراني الخاصة بها، وشدة مرونتها في تحمل التهديدات والحوادث السيبرانية (Lenka et al., 2023, p180) . علاوة على ذلك، يتعين على الشركات الإفصاح عن قدراتها في مجال حوكمة الأمن السيبراني، بما في ذلك إشراف مجلس الإدارة، ووصف دوره في تقييم وإدارة المخاطر السيبرانية، والخبرة ذات الصلة بهذه الإدارة، ودور الإدارة في تنفيذ سياسات وإجراءات واستراتيجيات الأمن السيبراني (Hetner, 2022, p3-4) .

ويتضح للباحث أن الشركات يجب أن تراعي الأهمية النسبية للمخاطر السيبرانية وهناك سبب للإفصاح عن مسؤولية مجلس الإدارة المتعلقة بالإشراف والرقابة على المخاطر السيبرانية، ويمكن إعطاء مسؤولية الإشراف و الرقابة على المخاطر السيبرانية إلى أي لجنة من لجان مجلس الإدارة.

ثالثاً: تحليل المعايير والأطر المحاسبية والتنظيمية للإفصاح عن المخاطر السيبرانية وإدارتها

شهد موضوع الإفصاح عن الأمن السيبراني اهتماماً كبيراً من قبل الهيئات المهنية المختلفة، من خلال إصدار العديد من الإرشادات والتقارير المهنية، لدعم إفصاح الشركات عن المخاطر االسيبرانية وكيفية إدارتها (Wang and Janvrinp1, 2019). وظهرت العديد من الأطر لمعالجة المخاطر والإفصاحات الأساسية للأمن السيبراني، ففي عام 2019، أصدر مركز أمن الإنترنت (CIS) الإصدار 7.1 من ضوابط CIS لتطوير وتنفيذ ضوابط الأمن السيبراني، وأصدر المعهد الوطني للمعايير والتكنولوجيا (NIST) إطاراً جديداً لمراقبة الأمن السيبراني (CIS, 2019 ; NIST, 2019) .

1- المعايير المحاسبية ذات الصلة بالإفصاح عن المخاطر السيبرانية

على الرغم من عدم وجود معيار محاسبي صريح يتناول المخاطر السيبرانية- حتى الآن- إلا أنه توجد بعض المحاولات للجهات المسؤولة عن إصدار المعايير المحاسبية، ومنها؛ بعض المناقشات التي تتناول قضايا الأمن السيبراني، وإصدار بعض التوصيات والتقارير الرسمية والإرشادات وأوراق العمل عبر مواقعها، ووضع الأمن السيبراني ضمن خطتها الإستراتيجية، وبعضها أصدر أطر طوعية للإفصاح عن إدارة المخاطر السيبرانية، ويتوقع **الباحث** أن إصدار معيار محاسبي للإفصاح عن الأمن السيبراني ومخاطره، ضرورة حتمية للحاق بالتطورات والمخاطر السيبرانية في البيئة الرقمية المحيطة، وفيما يلي عرضاً مختصراً لبعض المعايير المحاسبية ذات الصلة – من وجهة نظر الباحث- بالإفصاح عن المخاطر السيبرانية.

1/1- المعيار التحوطي - CPS 234 لأمن المعلومات

وصف مجلس معايير المحاسبة الأسترالي أن المخاطر المتعلقة بالأمن السيبراني وأمن البيانات وخصوصية العملاء، تحظى باهتمام مجتمع الاستثمار العالمي، الذي لاحظ أن الحوادث السيبرانية يمكن أن تعطل العمليات التجارية، وتقلل من قيمة محفظة الشركة وأرباحها (AASB, 2022, p4) . ويشمل نطاق معايير أو لوائح الأمن المادي و/أو السيبراني معايير ولوائح إلزامية وقابلة للتنفيذ تهدف إلى التخفيف من مخاطر الأمن المادي و/أو الأمن السيبراني المتعلقة بموثوقية و/أو مرونة البنية التحتية (AASB, 2022, p277) . وتتضمن آليات الإفصاح طبقاً المعيار في الإفصاح عن) :الأدوار والمسؤوليات المتعلقة بأمن المعلومات لمجلس الإدارة والإدارة العليا، مدى قدرة الكيان في الحفاظ على أمن المعلومات بما يتناسب مع حجم ومدى التهديدات التي تتعرض لها أصولها من المعلومات، بحيث تتيح استمرار التشغيل السليم للكيان، ومدى تنفيذ ضوابط الحماية لأصول المعلومات الخاصة به بما يتناسب مع مدى أهمية وحساسية أصول المعلومات) وإخطار APRA بحوادث أمن المعلومات الجوهرية APRA, CPS 234.item67, 2019, p24) .

2/1- المعايير الدولية ومعايير التقارير المالية ذات الصلة بالمخاطر السيبرانية:

إن المعايير المحاسبية هي الأساس للمحاسبين والإدارة لإبلاغ المستثمرين بالإنتهاكات، وينبغي على واضعي معايير المحاسبة وصانعي السياسات تقديم أدلة مهمة حول تنظيم الأمن وخروقات البيانات على وجه التحديد، والقواعد المتعلقة بإعادة النظر في مفهوم الأهمية النسبية بشكل عام وفيما يتعلق بانتهاكات البيانات وما يخالف إدارة المستثمرين ومتى تحدث هذه المعلومات (Juma'h and Alnsour, 2021, p14) . ويقضي **معيار المحاسبة الدولي** (IAS 1) في الفقرة (112) بأن توفر الإيضاحات المتممة للقوائم المالية معلومات إضافية، وخاصةً تلك التي لم يتم عرضها في صلب القوائم المالية ولكنها ذات صلة بفهم أي منها. وفي سياق المخاطر السيبرانية، ستكون المعلومات ذات صلة إذا كان المستثمرون يتوقعون بشكل معقول أن المخاطر السيبرانية لها تأثير كبير على الكيان وهذا من شأنه أن يؤثر على قرارات المستثمرين، وتتضمن المخاطر السيبرانية خصائص هامة يجب القياس

والإفصاح عنها لتقييم مبالغ وتوقيتات التدفقات النقدية المستقبلية، ومدى التأكد من ذلك وطبيعة ومدى ما تنطوي عليه من حقوق والتزامات متنوعة.

ويرى **الباحث** أن المخاطر السيبرانية تؤثر على الاعتراف والقياس المتعلقة بالبنود في البيانات المالية، ويجب على الشركات أن تعترف وتفصح عن أي انخفاض جوهري أو اضمحلال في القيمة أو تأثيرات أخرى في البيانات المالية، وقد يؤدي تطبيق تعريف **الأهمية النسبية** والمبادئ الواردة في المعيار المحاسبي (IAS 1) إلى انعكاس بعض المعلومات عن المخاطر السيبرانية في البيانات المالية.

وقد تحتاج المنشأة **لتفسير حكمها** بأنه لم يكن من الضروري إدراج المخاطر السيبرانية في افتراضات انخفاض القيمة، أو كيف تأثرت أو لم تتأثر تقديرات التدفقات النقدية المستقبلية المتوقعة، وقد تفكر الشركات في الإفصاح عن مدى تعرض استثماراتها أو محافظ قروضها للمخاطر السيبرانية، وقد تفصح المنشأة عن تقديراتها أو أحكامها التي تم إجراؤها حول المخاطر المتعلقة بالأمن السيبراني، وقد يشمل ذلك الإفصاح عن **الافتراضات** التي تم إجراؤها حول المخاطر السيبرانية في تقييم خسارة الانخفاض في القيمة للأصل المتضرر. ويتطلب **العرض العادل** من المنشأة أن تقوم بعرض إفصاحات إضافية عندما تكون المتطلبات الواردة في معايير المحاسبة غير كافية لتمكين المستخدمين من فهم تأثير معاملات معينة وأحداث وظروف أخرى (كالمخاطر السيبرانية) على المركز المالي للمنشأة وأدائها المالي، وإذا كانت الإدارة على دراية عند تقييمها لقدرة المنشأة على **الاستمرارية** بوجود عدم تأكد جوهري مرتبط بالأحداث السيبرانية المحتملة، قد يترتب عليها شك جوهري في قدرة المنشأة على الاستمرار فإنه يجب الإفصاح عن مظاهر عدم التأكد، وقد تهدد المخاطر السيبرانية فرض الإستمرارية، وتحتاج الشركة إلى أدلة أكثر لإثبات قدرتها على موجهة تلك المخاطر بالبيئة الرقمية المحيطة، بالقدر الذي يقلل عدم التأكد من استمراريتها في النشاط أم لا.

وورد بتقرير **مجلس معايير المحاسبة والمراجعة الأسترالي (AUASB)**، أنه في حالة وقوع حدث إلكتروني، تشمل بعض الأمثلة على التأثيرات المباشرة وغير المباشرة على التقرير المالي ما يلي: (الاعتراف بالمخصصات أو الإفصاح عن الالتزامات الطارئة نتيجة لخرق البيانات، وانخفاض قيمة الأصول بسبب انخفاض التدفقات النقدية التشغيلية نتيجة للهجوم السيبراني، والآثار العامة لقدرة الكيان على الاستمرار كمنشأة مستمرة) (AUASB, 2021, p5) . ووفقا للـAUASB يمكن أن يكون للمخاطر السيبرانية الأثار المباشرة وغير المباشرة على التقارير المالية من حيث (فريد، 2022، ص439) :

1- الاعتراف بالمخصصات أوالافصاح عن الالتزامات الطارئة نتيجة لخرق البيانات وذلك قد يكون نتيجة لغرامات أو عقوبات من المنظمين أو اتخاذ اجراءات قانونية من قبل الأطراف المتأثرة.
2- التغيير في القيمة العادلة للأصول نتيجة لحادث الكتروني فعندما يتم استهداف صناعة معينة أو تتعرض لأزمات أو مشكلات فقد يكون هناك تردد في التعامل مع كيانات داخل تلك الصناعة.
3- انخفاض قيمة الأصول بسبب انخفاض التدفقات النقدية التشغيلية نتيجة للهجوم السيبراني، حيث يؤدي إلى ايقاف العمليات لفترة طويلة من الوقت او قد يؤدي الى الحاق ضرر كبير بالعلامات التجارية.

ويرى الباحث أنه يجب إدخال تطوير لبعض أجزاء المعايير المحاسبية، لتتناسب مع التطورات الرقمية والتكنولوجيا الحديثة وكيفية معالجتها والاعتراف بها وبأية خسائر نتيجة التعامل من خلالها، مثل الأصول الرقمية والعملات الرقمية المشفرة التي يتم تداولها عبر المنصات الرقمية. وتأسيساً على ما سبق، نستعرض الجدول التالي **رقم (1)**، لتوضيح كيف يمكن للمخاطر السيبرانية بشكل خاص أن تؤثر- من وجهة نظر الباحث- على البيانات والتقارير المالية والمعايير المحاسبية التي قد تحتاج إلى النظر فيها.

جدول رقم (1)

تأثير المخاطر السيبرانية على التقارير المالية طبقاً للمعايير المحاسبية ذات الصلة

المعيار المحاسبي ذات الصلة	التأثير على التقارير المالية
IAS 16 الممتلكات والآلات والمعدات، و IAS 38 الأصول غير الملموسة	قد تؤثر **المخاطر السيبرانية** على كل مما يلي: - الأعمار الإنتاجية المقدرة للأصول، وبالتالي مقدار الإهلاك أو الإطفاء المعترف به كل سنة. - قد يكون أحد شروط الاستمرار في تشغيل بند من بنود الأصول التكنولوجية (مثل أجهزة الحاسب)، القيام بإجراء فحص بصفة دورية للكشف عن الأعطال والعيوب والفيروسات وتحديثها، وكلما قامت المنشأة بفحص من تلك الفحوص الرئيسية فإنها تعترف بتكلفة ذلك الفحص ضمن القيمة الدفترية للأصل كإحلال. - قد تؤدي المخاطر السيبرانية إلى إيقاف الاعتراف بالأصل غير الملموس عند انعدام توقع تحقق منافع اقتصادية مستقبلية من استخدامه نتيجة تلف أو تدمير الأصل غير الملموس. - الإفصاح عن الخسارة الناتجة عن الاضمحلال – بسبب الهجمات السيبرانية- التي تم الاعتراف بها في قائمة الدخل خلال الفترة، وخسائر الاضمحلال التي تم ردها للأرباح أو الخسائر أثناء الفترة.
IAS 24 الإفصاح عن الأطراف ذوي العلاقة	في ظل استخدام الخدمات الرقمية المفتوحة ومشاركة الشركات والبنوك المعلومات حول حسابات العملاء، والاستعانة بخدمات الطرف الثالث والمخاطر المتعلقة بها، وأيضاً في ظل التحالفات بين شركات التكنولوجيا، يجب أن يكون هناك إفصاحات معززة لبيان مدى تأثير المعاملات مع هذه الأطراف على القوائم والتقارير المالية، وعلى مدى تقييم عملياتها من جانب مستخدمي القوائم المالية وتقييم المخاطر والفرص والتحديات التي تواجهها نتيجة التعامل مع هذه الأطراف، وفي هذا الشأن يجب اتباع إرشادات معيار المحاسبة الدولي (IAS 24) "الإفصاح عن الأطراف ذوي العلاقة"، لتحديد مدى أهمية المعاملات مع هذه الأطراف من حيث الحجم، شروط المعاملات، مدى الإفصاح عنها، والتدابير المتخذة لتخفيض مخاطر التعامل مع هذه الأطراف.
IAS 36 انخفاض قيمة الاصول	- يمكن أن تكون القيمة الدفترية للأصول مثل الممتلكات والآلات والمعدات والأصول المعترف بها فيما يتعلق بالأصول غير الملموسة والشهرة وبراءات الاختراع والملكية الفكرية والبرامج، مبالغ فيها إذا كانت حسابات انخفاض القيمة لا تأخذ تأثير المخاطر السيبرانية في الاعتبار. - قد يكون تعرض المنشأة للمخاطر السيبرانية مؤشراً على أن أصلاً أو مجموعة أصول قد تعرضت لانخفاض القيمة، ويؤثر على التدفقات النقدية الداخلة والخارجة المقدرة المستخدمة في حساب المبلغ القابل للاسترداد. - عندما يكون للمخاطر السيبرانية تأثير كبير على عمليات الكيان، فإن المعلومات حول كيفية أخذ ذلك في الاعتبار في حسابات المبلغ القابل للاسترداد ستكون مناسبة لمستخدمي البيانات المالية.
IAS 37 المخصصات والالتزامات الطارئة والأصول المحتملة	- يمكن أخذ الشكوك المحتملة (حالات عدم التأكد) المتعلقة بالمخاطر السيبرانية، وما يحيط بها من أحداث في الحسبان عند تحديد أفضل تقدير للمخصص، وقد تكون الأحداث السيبرانية المستقبلية المتوقعة هامة عند قياس وتقدير المخصصات، ويجب الإفصاح عن الافتراضات الرئيسية التي تم إجراؤها حول الأحداث المستقبلية. **ويمكن أن يكون للمخاطر السيبرانية التأثيرات التالية:** - الاعتراف بشرط **عقد محملاً بالخسارة** المحتملة للإيرادات أو زيادة التكاليف في ظل حالات المخاطر السيبرانية؛ وهو العقد الذي تكون فيه التكاليف التي لا يمكن تجنبها للوفاء بالتزامات العقد أكبر من المنافع الاقتصادية المتوقع الحصول عليها . - **زيادة المخصصات** المعترف بها لإيقاف تشغيل الخدمة أو الوصول غير المصرح به. - الإفصاح عن المسؤولية المحتملة للتقاضي المحتمل والغرامات/ العقوبات. - **معالجة حالات الخسارة الطارئة:** باعتبار أن المخاطر السيبرانية غامضة بطبيعتها ويصعب تقديرها، فإن معالجتها تختلف بناءً على الدرجة لتي تكون فيها الخسارة محتملة، وفي بعض الحالات يكون الإفصاح في الإيضاحات المتممة كافياً. - وقد ينشأ عن المخاطر السيبرانية **التزامات محتملة** أو **التزام حالي** ينشأ عن أحداث سيبرانية في الماضي ولم يتم الاعتراف به لأنه لا يمكن قياس قيمته بطريقة يمكن الاعتماد عليها بصور كافية، ولا ينبغي على المنشأة الاعتراف بالالتزام المحتمل، و يتم الإفصاح عن الالتزام المحتمل وفقاً لما هو مطلوب في الفقرة (86). - **ويمكن القول بموجب هذا المعيار أن الحدث السيبراني الماضي الذي يقود إلى التزام حال يسمي حدث ملزم،** وحتى يكون الحدث ملزماً، فإنه من الضروري أن لا يكون للمنشأة أي بديل واقعي لتسوية الالتزام الناتج عن هذا الحدث وهذا يحدث فقط عندما: (تكون تسوية الالتزام تنفذ بالقوة الجبرية (عن طريق القانون)، وفي حالة وجود التزام حكمي عندما يكون الحدث (الذي ينتج عن أحد تصرفات المنشأة) يؤدى إلى خلق توقع لدى الأطراف الأخرى بأن المنشأة سوف تفي بالتزاماتها) .
IFRS 7 الأدوات المالية: الإفصاحات، IFRS 9 الأدوات المالية.	- تستخدم متطلبات انخفاض القيمة المعلومات التطلعية للتعرف على خسائر الائتمان المتوقعة، عند تحديد ما إذا كانت مخاطر الائتمان قد زادت منذ الاعتراف الأولي، ومراعاة أي تغييرات سلبية فعلية أو متوقعة في البيئة التكنولوجية المحيطة للمقترض والتي تؤدي إلى تغيير كبير في قدرة المقترض على الوفاء بالتزامات ديونه. - عندما تستثمر البنوك في مشاريع أو تقرض الأموال للشركات المتأثرة بالمخاطر السيبرانية، فإنها ستحتاج إلى النظر في كيفية تأثير التعرض للمخاطر السيبرانية على الخسائر الائتمانية المتوقعة لهذه القروض والاستثمارات، وعلى سبيل المثال، إذا كانت المنشأة معرضة بشكل كبير للتهديدات والحوادث السيبرانية لتقديمها خدماتها الإلكترونية والرقمية المفتوحة عبر الفضاء السيبراني، فيجب عليها تحديد مدى هذا التعرض وكيف يمكن للمخاطر السيبرانية أن تؤثر على المبالغ المعترف بها في بياناتها المالية.

	- يمكن لشركات التأمين والشركات المالية الاحتفاظ باستثمارات في الصناعات التي قد تتأثر بالمخاطر السيبرانية، وبالتالي ستكون معرضة لمخاطر الأسعار لهذه الاستثمارات، ويتطلب المعيار (IFRS 7) الإفصاح عن تعرض المنشأة للمخاطر الناشئة عن الأدوات المالية، ويمكن للمعلومات الكمية مثل تحليل الاستثمارات حسب الصناعة/ القطاع أن تحدد على وجه التحديد تلك القطاعات المعرضة للمخاطر السيبرانية وتشرح سياسة الكيان للحد من تعاملاتها مع تلك القطاعات.
IFRS 13 قياس القيمة العادلة	- يتطلب من المنشآت الإفصاح عن الافتراضات الرئيسية المستخدمة، عندما يتم الاعتراف بالأصول بالقيمة العادلة، وعندما تتأثر القيمة العادلة لأصل معين بالمخاطر السيبرانية، قد يحتاج الكيان إلى الإفصاح عن كيفية إدراج المخاطر السيبرانية في الحسابات، ويجب على الكيانات في القطاعات المتأثرة بالمخاطر السيبرانية الإفصاح عن افتراضاتها فيما يتعلق بالمخاطر السيبرانية، بغض النظر عن التأثير الكمي. - وفي حالة حدوث اضمحلال في القيمة العادلة، فإنه يتم الاعتراف بالخسائر الناتجة عن اضمحلال قيمة الاصول- بسبب التعرض للمخاطر السيبرانية- نتيجة أي تخفيض مبدئي ولاحق في القيمة العادلة للأصول، و يتم معالجة خسائر اضمحلال قيمة الاصول المعرضة للخطر السيبراني خصماً من القيمة الدفترية للاصول.
IFRS 15 الاعتراف بالإيراد من العقود مع العملاء	يتوقع **الباحث** أن تؤثر المخاطر السيبرانية على توقيت الاعتراف بالإيراد، وعند وجود عقد بين الكيان وطرف ثالث، تأخذ المنشأة في الاعتبار كلا من: **(أ) النتائج المترتبة على حدوث الخرق**، أي تأثير خرق شروط العقد على المركز المالي للمنشأة وأدائها المالي وتدفقاتها النقدية، وإذا كانت هذه العواقب ستؤثر على المركز المالي للمنشأة أو الأداء المالي أو التدفقات النقدية بطريقة يمكن توقعها بشكل معقول للتأثير على قرارات المستخدمين الأساسيين، فمن المحتمل أن تكون المعلومات حول وجود العقد وشروطه جوهرية ويتم الإفصاح عنه في القوائم والتقارير المالية، وعلى العكس من ذلك، إذا كانت عواقب خرق شروط العقد لن تؤثر على المركز المالي للكيان أو الأداء المالي أو التدفقات النقدية بهذه الطريقة، فقد لا تكون هناك حاجة إلى الإفصاحات حول شروط العقد **(ب) احتمالية حدوث خرق شروط العقد**، وكلما زاد احتمال حدوث خرق، زاد احتمال أن تكون المعلومات حول وجود وشروط العقد جوهرية، وسيؤثر على الوفاء بالتزامات العقد بين الأطراف المتعاقدة.

المصدر: الباحث، بناءً على تحليل بعض المعايير المحاسبية ذات الصلة.

3/1- معايير محاسبة الإستدامة وتقارير الأعمال المتكاملة ذات الصلة بالمخاطر السيبرانية:

قد **أصدر مجلس معايير محاسبة الإستدامة** (SASB) عام ٢٠١٤ معايير محاسبة الاستدامة مصنفة وفقا للقطاعات الاقتصادية ومنها معيار محاسبة الاستدامة رقم (FNO101) للحفاظ على خصوصية العملاء وأمن البيانات، والمقاييس والمخاطر والفرص المرتبطة بعملها والعمليات التي تقوم بها، بهدف توفير المعلومات التي تساعد في فهم ومعرفة مدى المساهمة في تحقيق التنمية المستدامة (SASB, 2014,101). ونشر **(SASB)** تقريراً وفقاً لمعايير الاستدامة لقطاع الخدمات المهنية والتجارية فيما يتعلق بالأمن السيبراني، ويوضح الجدول التالي **رقم (2)** استجابة لكل من مقاييس SASB :

جدول رقم (2)
موضوعات الإفصاح عن المخاطر السيبرانية في مقاييس مجلس معايير محاسبة الاستدامة

الموضوع	SASB CDE	المقاييس المحاسبية	استجابة الشركة
خصوصية البيانات	TC-TL-220a.1	وصف السياسات والممارسات المتعلقة بالإعلان السلوكي وخصوصية العميل.	ـــــــ
	TC-TL-220a.2	عدد العملاء الذين تُستخدم معلوماتهم لأغراض ثانوية، والنسبة المئوية للمشتركين	ـــــــ
	TC-TL-220a.3	إجمالي مبلغ الخسائر المالية نتيجة الإجراءات القانونية المرتبطة بخصوصية العميل.	ـــــــ
	TC-TL-220a.4	(1) عدد طلبات تنفيذ القانون للحصول على معلومات العميل، (2) عدد العملاء الذين تم طلب معلوماتهم، (3) النسبة الناتجة عن الإفصاح.	ـــــــ
أمن البيانات	TC-TL-230a.1	وصف النهج المتبع لتحديد ومعالجة مخاطر أمن البيانات، بما في ذلك استخدام معايير الأمن السيبراني لطرف ثالث.	ـــــــ
	TC-TL-230a.2	وصف والممارسات المتعلقة بجمع معلومات العملاء واستخدامها والاحتفاظ بها.	ـــــــ
	TC-TL-230a.3	(1) عدد انتهاكات البيانات، و (2) النسبة المئوية التي معلومات تجارية سرية للعملاء أو معلومات تعريف شخصية (PII)، و (3) عدد العملاء المتضررين (المتأثرين) .	ـــــــ

Source: (https://www.sasb.org/) 2021.

ومن أهم ما جاء بهذا المعيار وله علاقة بالإفصاح المحاسبي عن المخاطر السيبرانية هو المجال الثاني، والذي يتطلب الإفصاح عن مخاطر أمن البيانات وخصوصية العملاء والآليات والاستراتيجيات المتبعة لإدارة هذه المخاطر وحماية حقوق العملاء، حيث تعد حماية البيانات الشخصية للعملاء مسؤولية أساسية، وأن المؤسسات التي تفشل في

حماية هذه البيانات تكون معرضة لفقدان ثقة العملاء وبالتالي انخفاض الإيرادات، وبتحليل وتقييم هذا المعيار في ضوء متطلبات الإفصاح المحاسبي عن المخاطر السيبرانية يتضح للباحث أن المعيار اقتصر على الإفصاح عن مخاطر البيانات وأمن المعلومات دون غيرها من المخاطر الأخرى. وقد تضمن معيار (FN-CB) الصادر عن المجلس فقرات تتعلق بالأمن السيبراني، ويتضمن المعيار المؤشرات الآتية: (عدد الخروقات السيبرانية خلال فترة معينة، والنسبة المئوية التي تتضمن معلومات تعريف شخصية (معلومات تحديد الهوية الشخصية)، ونسبة الحسابات المصرفية المتأثرة بالهجمات السيبرانية، ووصف لإدارة المخاطر السيبرانية) (يعقوب وآخرون، 2022، ص 1411) .

ولتعزيز دور ودعم المبادرة **لتقارير الأعمال المتكاملة** للوحدات الاقتصادية في مجال معلومات الأمن السيبراني، والتي يجب الإفصاح عنها في ضوء تقارير أعمال الشركات، ويجب أن يكون للتقرير المتكامل أهمية خاصة في تقديم الأمن السيبراني والمخاطر السيبرانية، ويتمثل دوره في إيصال استراتيجية المنظمة، ونظام الحوكمة المعتمد ونتائج الأعمال وآفاقها إلى جانب العوامل الداخلية (Ferens, 2021, p40). وتماشياً مع المحتويات المقترحة للتقرير المتكامل، يُعتقد أن طريقة تأمين الأفراد ضد التهديدات السيبرانية يمكن وصفها في أجزاء مختلفة من التقرير المتكامل من خلال الجدول التالي **رقم (3)** كالتالي:

جدول رقم (3)
عناصر التقرير المتكامل والقضايا السيبرانية

عناصر التقرير المتكامل	الخصائص
معلومات عامة عن المنظمة	ماذا تفعل المنظمة وتحت أي ظروف تعمل؟ هل هي عرضة للهجمات في الفضاء السيبراني؟
حوكمة الشركات	كيف تدعم حوكمة الشركات قدرة المؤسسة على خلق قيمة على المدى القصير والمتوسط والطويل أيضاً فيما يتعلق بالتهديدات السيبرانية؟
نموذج الأعمال	ما هو نموذج عمل المنظمة؟ هل يأخذ في الاعتبار جوانب الأمن السيبراني؟
الفرص والمخاطر	هل هناك مخاطر تتعلق بالأمن السيبراني، وما هي الفرص التي ستؤثر على قدرة المنظمة على خلق قيمة على المدى القصير والمتوسط والطويل؟
الاستراتيجية	إلى أين تذهب المنظمة ؟ هل يشمل جوانب الأمن السيبراني ؟
الإنجازات	إلى أي مدى تريد المنظمة تحقيق أهدافها الاستراتيجية المحددة،وما هو أدائها من حيث التنفيذ والتأثير على رأس المال، بما في ذلك التهديدات السيبرانية؟
التوقعات ـ وجهات النظر	ما هي التحديات والشكوك التي قد تواجهها المنظمة في تنفيذ إستراتيجيتها للأمن السيبراني، وما الآثار المحتملة على نموذج أعمالها وأدائها المستقبلي ؟
أسس الإعداد والعرض	كيف تحدد المنظمة القضايا التي يجب معالجتها في التقرير المتكامل وكيف تحدد أو تقيِّم قضايا الأمن السيبراني؟

Source; own study based on IIRC ,2013, p 5; Ferens, 2021, p40-41.

كما يتضح من محتوى الجدول السابق، يمكن لمعايير GRI أن تعزز الإفصاح عن الأمن السيبراني على وجه التحديد مع معيار (GRI 418) لخصوصية العملاء، وقد تظهر المعلومات في أجزاء مختلفة من التقرير المتكامل، ويُعتقد أن تدابير الحماية من التهديدات السيبرانية يمكن وصفها أيضاً في **تقرير الإدارة** وتشمل معلومات حول: (الأحداث التي تؤثر بشكل جوهري على أنشطة المنشأة التي حدثت في السنة المالية، وبعد انتهائها حتى تاريخ الموافقة على البيانات المالية؛ والتطوير المتوقع للمؤسسة؛ والإنجازات الرئيسية في مجال البحث والتطوير؛ والأدوات المالية من حيث المخاطر (تغيرات الأسعار، مخاطر الائتمان، الاضطرابات الكبيرة في التدفقات النقدية وفقدان السيولة المالية التي تتعرض لها المنشأة بسبب التعرض للمخاطر السيبرانية) (Ramírez et al., 2022,p7) .

2- أطر الأمن السيبراني : الأطر هي مبادئ توجيهية عامة تغطي مجموعة واسعة من المجالات في المنشآت، ويحدد إطار العمل الأساسيات لتحقيق هدف معين، ويتم استخدام الإطار لتحديد معايير الجودة التي ينبغي تحقيقها، ووصف النطاق، وتلخيص الأهداف والنتائج (Taherdoost, 2022, p3) . وتم وضع أطر عمل معينة من قبل السلطات من أجل تقليل المخاطر السيبرانية (Kahyaoglu & Caliyurt, 2018, p362) . ويمكن تمييز العديد من هذه الأطر على أنها سياسات ونماذج وإجراءات السياسات الأمنية (Lois et al., 2021, p32) . وبعض أطر الأمن السيبراني إلزامية وبعضها الآخر يتم تشجيعه بقوة من قبل الجهات التنظيمية، والهدف الرئيسي لإطر الأمن السيبراني هو تقليل مخاطر التهديدات السيبرانية (Taherdoost, 2022, p8) .

1/2- إطار عمل COBIT 2019: تم تطويرCOBIT5من قبل جمعية مراجعة ومراقبة نظم المعلومات (ISACA)، ويعتبر إطار (COBIT) من أفضل الأطر في إدارة مخاطر تكنولوجيا المعلومات وتحقيق فعالية حوكمة تكنولوجيا المعلومات (عبيدالله وآخرون،2021، ص 56؛ فريد، 2022، ص437) . والذي يركز على إدارة المخاطر السيبرانية من خلال الامتثال لحوكمة وإدارة تكنولوجيا المعلومات الفعالة (عثمان، 2022، ص8) . وفي نوفمبر ٢٠١٨ تم إصدار النسخة الحالية من الإطار تحت مسمى COBIT 2019، ويهدف هذا الإطار إلى توفير مرونة أكبر في تنفيذ حوكمة تكنولوجيا المعلومات EGIT وتضمن هذا الإطار تعديل لمبادئ COBIT 5 (محروس, أبوالحمد، 2022، ص 448) . ويهدف إطار عمل COBIT إلى الجمع بين حوكمة الشركات وحوكمة تكنولوجيا المعلومات معاً، ويشمل إحدى أفضل الممارسات في مجال الحوكمة، ومراجعة نظم المعلومات الإلكترونية، والتكنولوجيات المتصلة، وحماية أمن المعلومات، ويشمل COBIT 2019 34 عملية رئيسية لتكنولوجيا المعلومات، أفضل الممارسات والنهج فيما يتعلق بالعمليات والبنية التحتية والموارد والمسؤولية وإدارة الرقابة(Serkan and Ahmet, 2022, p714; Shaker et al., 2023, p4) .

2/2- إطار عمل الأمن السيبراني (CSF) NIST و سلسلة SP800 القياسية: يستند الإطار إلى المعايير والمبادئ لتوجيه المنظمات في الممارسات التي تخفف من الآثار المحتملة للمخاطر السيبرانية (Lois et al., 2021, p32) . وتتناول عائلة أطر عمل NIST مجموعة متنوعة من المجالات، بما في ذلك خصوصية المعلومات وتقييمات المخاطر والأمن السيبراني لتسهيل جهود إدارة المخاطر (RM) في الأمن السيبراني والامتثال داخل المنظمات، لمساعدة المؤسسات على تحديد وتقييم وإدارة المخاطر السيبرانية، وتعبر هذه الوثيقة أفضل إصدارات NIST حتى الآن لدمج الأمن السيبراني في ادارة مخاطر المؤسسة، ومن ثم يمكن تطبيق المبادئ المقترحة وأفضل الممارسات لتحسين الأمن السيبراني والمرونة على جميع الشركات بغض النظر عن الحجم أو درجة المخاطر السيبرانية، علاوة على ذلك، فإنه يوفر لغة مشتركة لفهم وإدارة والتعبير عن المخاطر السيبرانية لجميع أصحاب المصلحة، ويمكن استخدامه للمساعدة في تحديد الإجراءات وتحديد أولوياتها للحد من المخاطر السيبرانية، وهي أداة لمواءمة السياسات والأعمال والأساليب التكنولوجية لإدارة مثل هذه المخاطر، ويمكن استخدامه لإدارة المخاطر السيبرانية عبر المؤسسات بأكملها أو يمكن أن يركز على تقديم الخدمات الهامة داخل المؤسسة (NIST, 2018; Jarjoui & Murimi, 2021, p147;Cao et al., 2023,).

ويساعد إطار عملNIST للأمن السيبراني المؤسسات على زيادة تدابير الأمن السيبراني الخاصة بها، ويوفر هيكلاً تنظيمياً متكاملاً للنهج المختلفة في الأمن السيبراني، من خلال جمع أفضل الممارسات والمعايير والتوصيات، ويوفر وسيلة فعالة للتعبير عن متطلبات الأمن السيبراني (Taherdoost, 2022, p9) . وتم تطوير سلسلة معايير SP800 بواسطة NIST وتتضمن سلسلة SP 800 القياسية مجموعة من المنشورات المختلفة، مثل إطار عمل إدارة مخاطر، وإطار عمل الأمن السيبراني NIST، و NIST SP 800-39، و NIST SP 800-53، وإطار عمل خصوصية NIST، و NIST SP 800-37 و SP800-12 و NIST SP 800-53R1 و NIST SP 800-14 و (NIST SP 800-30 (Hamdani et al., 2021, p6) . وتعمل NIST حالياً على تحديث إطار عمل الأمن السيبراني الحالي (CSF 2.0)، ويشير إطار العمل إلى **خمسة مجالات**، وهي: (تحديد أصول المنظمة وحمايتها وكشفها والاستجابة لها واستردادها)، ويساعد استخدام هذا الإطار المؤسسات على تحديد المجالات التشغيلية التي تتطلب الاستثمار والإنفاق في حماية الأمن السيبراني (NIST, 2023; Mierzwa and Klepacka, 2023, p30) .

ونستعرض صورة مختصرة لأهم الأطر ونناقش حدودها في سياق الأمن السيبراني على النحو التالي:-

- **المعيارNIST SP 800-53 :** يركز هذا المعيار بشكل أساسي على الخصوصية والضوابط في أنظمة المعلومات وفي المؤسسات التي تهدف إلى تأمين الأصول والأفراد والعمليات من التهديدات السيبرانية المختلفة، بما في ذلك الأخطاء البشرية والهجمات العدائية والفشل في العمليات، والكوارث الطبيعية، ومخاطر الخصوصية والتهديدات من خارج الكيان (Karie et al., 2021,p121979) .
- **المعيارNIST SP 800-14 :** يتم وصف مبادئ الأمن الشائعة الاستخدام في هذا المعيار، لمساعدة المستخدمين على تحقيق السياسات في مجال الأمن السيبراني، ويزود المنظمات بالمتطلبات التي ينبغي أن تتبعها لتأمين موارد تكنولوجيا المعلومات، ويضمن توظيف للمنظمات جاهزية حلول أمن تكنولوجيا المعلومات في حالة التهديدات السيبرانية (Hamdani et al., 2021, 14;Taherdoost, 2022, p11) . ومن المهم أن تنفذ المؤسسات إطار عمل NIST مع الاستمرار في تقييم بنيتها التحتية الحالية باستخدام تحليل التكلفة والعائد (Gordon et al.,

2020) . ويجب تقييم تنفيذ أطر عمل واستخدامها من قبل المنظمات بناءً على مستوى نضج المخاطر وتحليل التكلفة والعائد (Alshar'e, 2023; Mierzwa and Klepacka, 2023, p33) .

3/2- سلسلة ISO/ IEC 27000 للمنظمة الدولية للتوحيد القياسي (ISO): تم تطوير سلسلة ISO 27000، والتي تتناول المعايير التي تمكن المؤسسات من تنفيذ العمليات والضوابط لدعم مبادئ أمن المعلومات، ويتمثل الاعتبار الرئيسي لمعايير ISO 27000 في تحقيق الأهداف الإدارية والتنظيمية والأهداف الفرعية من خلال التأكيد على مناهج المخاطر، وتتوفر إرشادات للتنفيذ المستند إلى المخاطر لإدارة المخاطر السيبرانية في ISO/ IEC 27005، وتدعم المفاهيم والمتطلبات المدرجة ومنها على سبيل المثال، أمن المعلومات والأمن السيبراني وحماية الخصوصية (ISO/IEC 27007: 2020)، وأمن المعلومات والأمن السيبراني وحماية الخصوصية- متطلبات تطبيق خاص بقطاع معين (ISO/IEC 27009: 2020)، وأمن المعلومات والأمن السيبراني وحماية الخصوصية- حوكمة أمن المعلومات (ISO/IEC 27014: 2020)، وتكنولوجيا المعلومات- الأمن السيبراني- نظرة عامة ومفاهيم (ISO/IEC TS 27100:2020)، وتكنولوجيا المعلومات والأمن السيبراني وحماية الخصوصية- إرشادات تطوير إطار عمل الأمن السيبراني (European) (ISO/IECTS 27110:2021 Commission, 2021, p28-30; Thamrongthanakit, 2023, p2) .

وأشارت دراسة (شحاتة، والبردان، 2021، ص 14) إلى أنه في حال وجود اتفاقيات أو إلتزامات دولية معتمدة محلية تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجهة الالتزام بتلك المتطلبات، من خلال التأكيد على أهمية تعزيز الأمن السيبراني من خلال وضع معايير واضحة ومعتمدة من قبل المؤسسات، واتخاذ إجراءات فعالة للالتزام بها، وتتمثل **معايير تعزيز الأمن السيبراني** في: (حماية وتشفير البيانات والمعلومات، وحماية وإدارة الأصول والأنظمة، وإدارة الثغرات واختبارات الاختراق، ومراقبة الأمن السيبراني، وإدارة حوادث وتهديدات الأمن السيبراني، وإدارة أمن الشبكات والنسخ الاحتياطية) . ويضمن ISO/ IEC التناغم بين السرية والنزاهة والاستمرارية لتحقيق أمن المعلومات داخل المنظمة، ويتتبع هذه الخطوات: (تحديد الأصول والتهديدات والتدابير القائمة، والإيضاحات وكشف النتائج المتوقعة، وتحديد المخاطر وتقديرها Serkan and Ahmet, 2022, p714) .

رابعاً: تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال

تحظى تكلفة رأس المال بأهمية كبيرة في الفكر المحاسبي والواقع العملي، باعتباره من أهم العناصر الأساسية لنجاح المنشأة واستمرارها بالسوق، وتؤثر بشكل مباشر على قيمة الشركة، فإذا حققت الشركة عائداً أكبر من تكلفة رأس المال، فإنه يتوقع أن تزداد القيمة السوقية لأسهمها (الوكيل، 2022، ص 679) . وتعتبر من أهم المحددات التي تستخدم في تقييم قدرة الشركات على استثمار أموالها (الزهيري, وآخرون، 2022، ص181) . بما يجعل الشركات أكثر قدرة في التعامل مع تبعات أي أزمة (النعيمي، ٢٠٢١، ص197) . ويعكس هيكل رأس المال تركيبة الدين أو الملكية في هيكل تمويل الشركات، ويؤثر اختيار المزيج التمويلي على تكلفة رأس المال وقيمة الشركة (السيد, وآخرون، 2023، ص55) .

1- مفهوم وأهمية تكلفة رأس المال

تمثل تكلفة رأس المال المتوسط المرجح للعائد الذي يطلبه المستثمرون، إذا امتلك مستثمر واحد المحفظة الكاملة للأسهم والديون الصادرة عن البنك، فإن تكلفة رأس المال ستكون هي العائد الذي يتوقع هذا المستثمر الحصول عليه، ويعكس المستوى العام للمخاطر (Dick-Nielsen et al., 2022, p2589) . ويقصد بها المعدل الذي ينبغي تحقيقه من استخدام الأصول المملوكة للشركة سواء تم تمويلها عن طريق المساهمين أو الدائنين (الصاوي، 2022، ص 72؛ Ezat, 2019, p370) . ويمكن تعريفها بأنها التكلفة التي يفرضها أصحاب الديون على الشركة، وحاملي الأسهم في مقابل الأموال الأساسية، ويتكون من عنصرين: تكلفة الدين وتكلفة حقوق الملكية، ويمثل هذان المكونان هيكل رأس مال الشركة (Rasheed, 2023, p7) .

ويمكن تعريفها بأنها شرط عائد المستثمرين لتحويل رأس المال إلى الشركات، ولذلك، يمكن أيضاً اعتبارها تكاليف تمويل للشركات (Knipp and Zimmermann, 2021, p8) . وتكلفة رأس المال في البنوك هي مدخلات في القرارات المتعلقة بكميات الإقراض والتسعير وكذلك القرارات المتعلقة بتخصيص الموارد لخطوط الأعمال المختلفة (Kovner and Van Tassel, 2022, p1349) .

ويخلص الباحث مما سبق إلى أن هناك تفسيرات مختلفة من وجهات نظر مختلفة، فيما يتعلق بمفهوم تكلفة رأس المال، فمن منظور **المنشأة**، فإن تكلفة رأس المال هي الحد الأدنى لمعدل العائد الذي يجب على الشركة تحقيقه قبل

أن تخلق قيمة، ومن وجهة نظر **المستثمرين**، يعد هذا تقييماً لمخاطر أسهم الشركة، ومن وجهة نظر **اقتصادية**، هي تكلفة الفرصة البديلة للاستثمار في الشركة، ولذلك يري **الباحث** أنه يمكن تعريف تكلفة رأس المال بأنها معدل العائد المطلوب تحقيقه من قبل المستثمرين علي استثماراتهم في المنشأة، وتعويضهم عن المخاطر المرتبطة بأنشطة وعمليات الشركة، وتمثل التضحية أو التكلفة التي يجب أن تدفعها المنشأة للمساهمين، والمقرضين مقابل الحصول على الأموال المطلوبة لتمويل أعمالها وممارسة أنشطتها.

2- عناصر تكلفة رأس المال:

يشير موضوع هيكل رأس المال، الذي نوقش على نطاق واسع في أدبيات المحاسبة المالية والتمويل، إلى تكلفة الديون (قصيرة وطويلة الأجل)، وتكلفة حقوق الملكية (الأسهم العادية والأسهم الممتازة والأرباح المحتجزة) الذي تستخدمه الشركة لتمويل استثماراتها (Eça and Albanez, 2022, p2). وتتأثر تكلفة رأس المال بمزيج الهيكل من الأموال المملوكة والمقترضة، ونسبة كل عنصر منها، ولكل مصدر تكلفته ومخاطره الخاصة، ويشير هيكل التمويل الأمثل إلى خفض تكلفة رأس المال إلى الحد الأدنى، وتشمل **شقين** أساسيين، وهما كالتالي:

1/2- تكلفة حقوق الملكية Cost of Equity (CE):

يستخدم المستثمرون تكلفة حقوق الملكية لتقييم فرص الاستثمار، ويمكن اعتبار تكلفة حقوق الملكية على أنها معدل العائد الذي يجب دفعه مقابل حقوق الملكية، وبالتالي تمثل التعويض الذي يطلبه السوق مقابل امتلاك الأصل وتحمل مخاطر الملكية، وغالباً ما يشار إلى هذا المقياس على أنه مقياس للمخاطر لأنه يوفر للمستثمرين إحساساً بتصور السوق للمخاطر (Dow et al., 2017, p19; Alia and AbuSarees, 2023, p4) . ويعرفها (Jiménez and Grima, 2020, p6) بأنها النسبة المئوية لمعدل العائد للحصول على القيمة السوقية للأصل عن طريق خصم أرباح التدفقات النقدية المستقبلية.

2/2- تقييم تكلفة الديون Cost of Debts (CD) في ضوء المعايير المحاسبية:

تتمثل تكلفة الديون في القروض قصيرة وطويلة الأجل والسندات، وهي المعدل الفعلي للعائد الذي تتحمله الشركة، من أعباء مالية مرتبطة بديونها الحالية التي تدفعها للمقرضين والمستثمرين، بعد أخذ الأثر الضريبي للفائدة أي بعد استبعاد الوفورات الضريبية (Amenya and Fon, 2022,p26) . وعرفها كل من (Kovner and Van Tassel, 2022, p1348; Bendriouch et al., 2022,p4) بأنها المتوسط المرجح لمدة سنة لمصروفات الفائدة السنوية على إجمالي الدين الذي يشمل الودائع (إذا كانت متوفرة) .

ويهدف معيار المحاسبة الدولي **(IAS 23)** ونظيره المصري **رقم (14)** ؛ إلى تحديد المعالجة المحاسبية لتكاليف الاقتراض؛ ويتطلب معالجة تكاليف الاقتراض كمصروفات، ويسمح المعيار برسملة تكلفة الاقتراض التي ترجع مباشرة إلى اقتناء أو إنتاج أو إنشاء أصل مؤهل لتحمل تكلفة الاقتراض، وعرفها بأنها "الفائدة وغيرها من التكاليف الأخرى التي تتحملها المنشأة فيما يتعلق باقتراض الأموال" (البراشي، 2022، ص57) . وتشكل تكاليف الاقتراض التي تنسب مباشرة إلى اقتناء أو إنشاء أو إنتاج أصل مؤهل جزءًا من تكلفة ذلك الأصل، ويتم الاعتراف بتكاليف الاقتراض الأخرى كمصروف (IFRS, 2022; Fischer, 2022, p16) .

وتتمثل المعالجة المحاسبية لتكلفة الديون وفقاً للمعيار الدولي ونظيره المصري على النحو الآتي:

- **المعالجة القياسية:** طبقاً للمعالجة القياسية فإنه يتم اعتبار تكلفة التمويل بالاقتراض كمصروفات، تحمل على الفترة التي تكبدت فيها المنشأة هذه التكلفة، بغض النظر عن كيفية استخدام القروض.

ويرى **الباحث** أن مبدأ تحميل كل فترة محاسبية بنصيبها من المصروفات غير عادل، حيث أن مبلغ القرض قد يكون كبيراً في سنواته الأولى، ثم يبدأ في التناقص في السنوات التالية، وقد تم إلغاؤها في المعيارين الدولي والمصري وفقاً للتعديلات الصادرة بموجب القرار الوزاري رقم 110 لسنة 2015.

- **المعالجة البديلة المسموح بها:** طبقاً للمعالجة البديلة المسموح بها، فإنه يتم إضافة تكلفة التمويل بالاقتراض المتعلقة مباشرة باقتناء أو إنشاء أصل وإنتاجه إلى تكلفة هذا الأصل، ويتم رسملة تكلفة التمويل بالاقتراض ضمن تكلفة الأصل، عندما يكون متوقعاً أن يتسبب في خلق منافع اقتصادية مستقبلية للمنشأة، وتكون هناك إمكانية لقياس التكلفة بشكل يمكن الاعتماد عليه.

ويتفق الباحث مع المعالجة البديلة التي توصي برسملة تكلفة التمويل بالاقتراض ضمن تكلفة الأصل، لأنها تتفق مع مفهوم التكلفة التاريخية للأصل، والتي تتضمن كافة التكاليف الضرورية التي تنفق على الأصل حتى

يصبح صالحاً للاستخدام، ويترتب على هذه المعالجة تحقيق مبدأ مقابلة الإيرادات بالمصروفات، ومن خلال تحليل متطلبات الاعتراف وفقاً للمعيار، يتضح للباحث أن يتم الاعتراف بالقروض التي تحصل عليها الشركة أو البنك بالقيمة العادلة أولاَ ناقصاً تكلفة الحصول على القرض، ويقاس القرض لاحقاً بالتكلفة المستهلكة، ويتم تحميل قائمة الدخل بالفرق بين صافي المتحصلات وبين القيمة التي سيتم الوفاء بها على مدار عمر القرض باستخدام طريقة العائد الفعلي.

3- تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال

وفقاً **لنظرية الإشارة**، يمكن استخدام حادثة خرق البيانات كإشارة تساعد المستثمرين على تقليل عدم تناسق المعلومات لديهم، حول قدرة الشركات على حماية بياناتها القيمة (Dong et al., 2022,p17) . وإن الشفافية الواسعة تتيح الاستفادة من التكلفة المنخفضة لرأس المال (Salvi et al., 2022) . ونظراً لأن سوق الدين الخاص يوفر غالبية التمويل الخارجي للشركات المتداولة في البورصة، فمن المهم فهم كيفية استجابة المقرضين للمخاطر السيبرانية عند التفاوض على القروض(Sheneman, 2022, p1) .

1/3- تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة حقوق الملكية:

استكشفت **نظرية التمويل** على نطاق واسع النزاعات المتأصلة بين أصحاب الديون وأصحاب الأسهم، وتثير الحجة حول ما إذا كان خرق الأمن السيبراني يؤثر على تكلفة رأس مال الديون تساؤلات حول ما إذا كان خرق الأمن السيبراني يؤثر في نفس الوقت على تكلفة حقوق الملكية. ولاختبار ذلك، أتبع Sheneman, 2017, p30, 32) واستخدم نهج دراسة الأحداث لتقدير تأثير الخرق على تكلفة حقوق الملكية، وتم قياس النسبة المئوية للتغيرات النسبية في حقوق الملكية بعد شهر وثلاثة وخمسة أشهر من خرق الأمن السيبراني، وبلغ متوسط الزيادات (2.3%، و4%، و3.9%) في تكلفة حقوق الملكية على التوالي.

ويمكن أن يؤدي الخرق الأمني إلى حث المستثمرين في الأسهم على تغيير تقييمهم للمخاطر لقدرة الشركة على توليد التدفقات النقدية المستقبلية، وبالتالي، قد يحتاجون بدورهم إلى عوائد أكبر في رأس المال، وترتبط الانتهاكات الأمنية بزيادة تكلفة حقوق الملكية من خلال زيادة المخاطر المنتظمة، وتتأثر تكلفة حقوق ملكية الشركات بشكل أكثر حدة عندما تحقق مؤشرات سوق الأسهم عوائد سلبية (Malliouris &Simpson , 2020, p2, 19) . وتوصلت دراسة (Abdollahi et al., 2022) إلى أن مخاطر المعلومات لها تأثير إيجابي كبير على تكلفة حقوق الملكية، وإن تأثير مخاطر المعلومات على عوائد الأسهم ليس ذا دلالة إحصائية. وذلك على عكس نتائج دراسة (Elmawazini et al., 2023)، التي توصلت إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال كمقياس لمخاطر المساهمين.

وتساعد إجراءات تخفيف التعرض للمخاطر السيبرانية في تقليل تكلفة حقوق الملكية، وتحفز على الاستثمار في الأمن السيبراني **لعدة أسباب** وهي كالتالي: **الأول**، تشير الأدبيات إلى أن المخاطر السيبرانية هي عامل خطر سعري مميز، وأن المساهمين يطالبون بمعدل عائد أعلى (أي ارتفاع تكلفة حقوق الملكية) للشركات ذات التعرض الأكبر للمخاطر السيبرانية (Jiang et al., 2022; Florackis et al., 2023) . وبالتالي، إذا نظر المساهمون إلى الشركات ذات التعرض الأكبر للمخاطر السيبرانية على أنها أكثر خطورة، فإن ذلك يترتب عليه أن الشركات التي تقلل من التعرض للمخاطر السيبرانية تتمتع بانخفاض في تكلفة حقوق الملكية (Ashraf & Sunder , 2023, p14) . **والثاني**، غالباً ما لا تعطي الشركات الأولوية للاستثمارات في الأمن السيبراني، على الرغم من أن مثل هذه الاستثمارات يمكن أن تقلل من تعرضها للمخاطر السيبرانية، وقد لا يتحمل المديرون دائماً تكاليف ضعف الأمن السيبراني بسبب التوقيت غير المتوقع للحوادث السيبرانية، ويجب أن يقلل الانخفاض الناتج في التعرض للمخاطر السيبرانية، من خلال استثمارات الشركة في الأمن السيبراني، إلى تقليل تكلفة حقوق الملكية (Ashraf and Sunder , 2023, p15) . **والثالث**، ينص إطار عمل **(NIST)** للأمن السيبراني على أنه ينبغي على الشركات تطوير وتحديث فهم عميق لبيئة الرقابة الداخلية الخاصة بها قبل أن تتمكن من تطوير استراتيجيات فعالة للأمن السيبراني، وبالتالي تقليل مخاطر المساهمين وتقليل تكلفة حقوق الملكية (Ashraf and Sunder , 2023, p16)

2/3- تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة الديون

يعتقد (Sheneman, 2017) أن تكلفة الديون هي مقياس قوي لتقييم حوادث خرق الأمن السيبراني؛ **أولاً**، تعتمد أسواق الديون بشكل كبير على معلومات البيانات المالية، وخاصةً سوق القروض الخاصة، التي تتعامل مع أكثر من 50٪ من تمويل الديون في الولايات المتحدة، **وثانياً**، بسبب هيكل السداد للديون، يتجنب الدائنون المخاطرة، مما

يحفزهم على فحص مخاطر المدين، **وثالثاً**، عناصر قياس تكلفة الدين متاحة بسهولة ومحددة في اتفاقيات القروض المتفاوض عليها. وبناء على ذلك، فإن تكلفة قياس الديون لها في جوهرها ضوضاء أقل من قياس تكلفة رأس المال المستقر (حقوق الملكية) . ويعد الإفصاح عن مخاطر الأمن السيبراني مفيداً للمستثمرين والدائنين، لأنه يمكن أن يكشف عن نقاط ضعف الرقابة الداخلية في بيئة الرقابة العامة للشركة بشكل عام، بالإضافة إلى فعالية الضوابط الداخلية المتعلقة بموثوقية البيانات المالية على وجه الخصوص (Li et al., 2018; Calderon and Gao, 2021; Harris et al., 2023, p193) .

واستناداً إلى **فرضية التعاقد المكلفة**، فإن عقود القروض تنشئ عهود لمنع المقترضين من الإجراءات التي تقلل من قيمة مطالبات المقرضين، ومن الممكن أن تقيد عهود القروض سلوك المدينين، سواء في حماية الدائنين من الخسائر أو تقليل تكاليف المخاطر المعنوية (Sheneman, 2017) . تعتبر تعهدات القروض بدائل للمراقبة المباشرة، حيث أن انتهاكها يمكن أن يؤدي إلى نقل حقوق السيطرة من المدينين إلى الدائنين عند الانتهاك (Dyreng et al., 2017) . ويمكن للدائنين استخدام معلومات المدين للتنبؤ باحتمالية حدوث خرق للأمن السيبراني وتسعيرها، بالإضافة إلى ذلك، قد يحاول المقرضون تنويع انتهاكات الأمن السيبراني المحتملة عبر محافظ قروضهم (Sheneman, 2017) . وتعترف **نظرية التعاقد غير المكتمل** بأنه ليس من الممكن للمقرضين والمقترضين التعاقد على القروض بنفس الشروط، في جميع الدول المحتملة في العالم لأن بعض المعلومات غير معروفة، ويتم تضمين هذه المعلومات غير الكاملة والمعرفة المستقبلية غير الكاملة في تسعير رأس المال، لأنه حسابه يعتمد على النتائج المحتملة المتوقعة، والتدفقات النقدية، وتقييم المخاطر(Harris et al., 2023, p195) .

وتتحمل الشركات التي تم خرقها فروق قروض بنكية أعلى ومتطلبات أكثر للضمانات والتعهدات Huang and (Wang, 2021) . وأن حملة السندات يفقدون ما يقرب من 2٪ من ثروتهم في غضون شهر بعد الهجوم السيبراني (Iyer et al., 2020) . ولقد توصلت دراسة (Harris et al., 2023, p208) أنه مع انخفاض جودة إفصاح الشركات عن مخاطر الأمن السيبراني في تقارير (K-10)، تزداد تكلفة الديون على هذه الشركات. على عكس دراسة (Vincent and Trussel, 2019, p495) التي توصلت إلى أن الإفصاح عن المخاطر السيبرانية لا تؤثر بشكل جوهري على مستوى تكلفة تمويل الديون.

ومن المحتمل أن يكون لخرق الأمن السيبراني تأثير سلبي جوهري على أعمال المقترض ويزيد من تكلفة الدين **بطريقتين، وهما**: (زيادة تكاليف مراقبة عمليات المقترضين؛ والتغييرات في تقييم مخاطر الائتمان (Sheneman, 2017, p3) . وتواجه الشركات التي تتعرض لهجمات سيبرانية زيادة في تكلفة الديون، وانخفاض في عدد المقرضين الذين يقدمون تمويلاً للديون الخاصة، وانخفاض حجم القرض (Sheneman, 2022, p6) . وبالمثل، حقق (Collins ,2019) في علاقة شدة خرق البيانات بعواقب ما بعد الخرق، وتوصل إلي أن الشركات التي تعرضت للخرق اضطرت إلى تحمل ديون إضافية كبيرة لدفع التكاليف الناتجة.

وفيما **يتعلق بتأثير العدوي**؛ إذا قام المقرضون بتعديل التوقعات بشأن المخاطر السيبرانية على مستوى قطاع معين بناءً على الهجمات السيبرانية بين االشركات، فمن المحتمل أن يكون هناك تأثير عدوى حيث يواجه المقترضون غير المخترقين فروقاً أعلى في القروض(Sheneman, 2022, p1) . وإذا قدمت الهجمات السيبرانية إشارة سلبية للمقرضين بأن المخاطر السيبرانية المتعلقة بالصناعة أعلى مما توقعه المقرضون، فمن المرجح أن يزيد المقرضون تكلفة الديون لتلك الصناعة (Files and Gurun, 2018) .

وفيما يتعلق **بمردود ادارة المخاطر السيبرانية**. فقد أشار (Havakhor et al., 2021)إلي أن الافصاح عن إدارة المخاطر السيبرانية من شأنه الحد من عدم تماثل المعلومات، ويقلل من تكلفة التمويل بالإقتراض. وقد يؤدي المزيد من الاستعداد للأمن السيبراني إلى توقع الدائنين إدارة أكثر ملاءمة للمخاطر السيبرانية، من خلال زيادة شفافية المعلومات من خلال الإفصاح عن المخاطر السيبرانية، وقد تؤدي زيادة الوعي بالأمن السيبراني إلى انخفاض تكلفة الديون للشركات، وتحسين شروط التعاقد على الديون، وقد يقيم الدائنين بشكل إيجابي التدابير والاجراءات الاحترازية للشركات لإدارة المخاطر السيبرانية (Godoy, 2021, p70, 75).

3/3- تحليل العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال (تكلفة حقوق الملكية و الديون) .

تعتبر معاملات تمويل الشركات مصادر جذابة للمعلومات لكثيرمن الأطراف، ويجب على جميع الشركات أن تكون على دراية بهذه المخاطر السيبرانية (ICAEW, 2017). ويدرك المستثمرون في حقوق الملكية والديون ارتفاع المخاطر السيبرانية ويتفاعلون مع الإفصاح عنها(Chen et al., 2022, p6). وإن المعلومات الإضافية

تقلل من عدم التأكد لدى المستثمرين، وبالتالي تقلل تكلفة رأس المال، ويؤدي عدم الافصاح عن معلومات موثوقة إلى خلق مشكلة عدم تناسق المعلومات، وهو ما يؤثر على تكلفة رأس المال (Bhatia & Kaur, 2023, p4) .

وبالنسبة لتأثير الإفصاح عن الأمن السيبراني على نتائج الشركات المختلفة، فرغم أن هناك المزيد من الأبحاث في هذا المجال، إلا أن النتائج غير حاسمة حتى الآن، حيث تفترض الأدبيات المستندة إلى عدم تناسق المعلومات بين المطلعين على الداخل والأجانب فيما يتعلق بمستوى المخاطر السيبرانية وإدارة الأمن السيبراني، هي أن الشركات قد يكون لديها حوافز للافصاح عن معلومات الأمن السيبراني لتقليل عدم تناسق المعلومات مع أصحاب المصلحة، واستناداً إلى **نظرية الوكالة**، يكون لدى المطلعين مزيد من المعلومات حول المخاطر السيبرانية التي تواجهها الشركة، وحول استراتيجيات الإدارة والتخفيف المتخذة فيما يتعلق بالمخاطر السيبرانية، وللتخفيف من عدم تناسق المعلومات، يكون لدى الشركات حوافز للافصاح عن هذه المعلومات لأصحاب المصلحة مثل المستثمرين والدائنين (Jensen & Meckling, 2019; Firoozi & Mohsni, 2023, p9) . وفي نفس السياق، تفترض **نظرية الإشارة** أن الشركات تستخدم الافصاح عن الأمن السيبراني للإشارة إلى التزاماتها بأمن المعلومات، خاصةً عندما تكون هي أو شركة نظيرة هدفاً للهجوم السيبراني، **وبناءً على هذه الأطر النظرية**، هناك حوافز كبيرة للشركات للافصاح عن المعلومات المتعلقة بالأمن السيبراني لأصحاب المصلحة لتقليل تكلفة رأس المال، ومنع الدعاوى القضائية، ومنع فقدان العملاء (Kelton and Pennington, 2020; Firoozi and Mohsni, 2023, p10) . وهذا الافصاح بدوره يزيد من القيمة السوقية، حيث أن الشركات التي تفصح عن المزيد من تدابير التخفيف المتعلقة بأمن المعلومات تكون أقل عرضة للحوادث السيبرانية المستقبلية (Gordon et al., 2018, Berkman et al., 2018) .

ومن منظور التمويل، يمكن أن تؤدي إخفاقات التحكم التشغيلي للأصول إلى زيادة تكلفة رأس المال بسبب عدم التأكد الإضافي بشأن التدفقات النقدية والأرباح المستقبلية(Sheneman, 2017, p6) . وإن ضعف الشفافية السيبراني يقلل ثقة المستثمرين ويؤثر سلباً على تكلفة رأس المال (SecurityScorecard et al., 2021,p3) . ومن **منظور أوسع**، تصبح أسواق رأس المال أقل كفاءة بالنظر إلى أن عملية اكتشاف السعر العادل للمستثمرين، وتعوقها الانتهاكات الأمنية التي تحدث تغييرات في تكلفة رأس المال، ونظراً لأن تكاليف رأس المال مرتبطة بشكل منهجي بالرافعة المالية للشركة، فمن المرجح أن تقوم الشركات المخترقة بتعديل هيكل رأس المال بعد الخرق(Malliouris and Simpson , 2020, p21, 24) .

ويمكن أن تؤدي الإفصاحات المتعلقة بالأمن السيبراني للشركة أيضاً إلى تقليل عدم تناسق المعلومات بين إدارة الشركة ومستثمريها، وهذا يمكن أن يقلل من تكلفة رأس مال الشركة (Lenka et al., 2023, p175) . وهو ما توصلت إليه نتائج دراسة (Elmawazini et al., 2023)، التي أكدت إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال كمقياس لمخاطر المساهمين.

على عكس بعض الدراسات مثل (الأمير، 2022، ص495؛ McGrath et al., 2022, p9)، والتي توصلت إلى أن الإفصاح عن المخاطر السيبرانية قد يؤدي إلى زيادة تكلفة رأس المال وكشف المعلومات السرية للمنافسين. وبسبب الإفصاح المقيد للشركات التي تم اختراقها، تؤدي إلى زيادة تكلفة رأس المال، من خلال تفاقم عدم تناسق معلومات السوق، وزيادة الرافعة المالية، ويمكن خفضها عن طريق زيادة حقوق الملكية أو تقليص الديون (Ali et al., 2022, p24-25, 37) . وقد تضعف الهجمات السيبرانية قدرة البنك على خدمة الدائنين الحاليين، في حالة عدم توفر المدفوعات أو الحسابات، وتزداد هذه المشكلة تعقيداً بسبب مشاكل المعلومات غير المتماثلة، ولديها القدرة على شل حركة رأس المال والسيولة (Eisenbach et al., 2022, p813) .

خامساً: الدراسة التطبيقية واختبارات الفروض

1- منهجية الدراسة التطبيقية

تتحقق 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:**

1/1- هدف الدراسة التطبيقية:

يتمثل الهدف العام للدراسة التطبيقية في قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك والمقترض، وذلك بالتطبيق على قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات، خلال السنوات المالية 2017إلى 2022، **ولذلك يشتق من هذا الهدف أهداف فرعية هي:**

- تحليل المحتوي الوصفي للتقارير المالية المنشورة الكترونياً لشركات العينة خلال السنوات المالية 2017إلى 2022وذلك لتحليل وتقييم مستوى الإفصاح عن المخاطر السيبرانية، وذلك بالاعتماد على مؤشر مقترح من الباحث لقياس الإفصاح عن المخاطر السيبرانية، وقياس درجة التفاوت (التمايز) بين شركات العينة عند الإفصاح عن المخاطر السيبرانية.
- قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك وذلك لشركات عينة الدراسة.

2/1- 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 عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات.
- **الفرض الثانى:** يوجد ارتباط معنوي بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض والمملوك.
- **الفرض الثالث:** يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك.

3/1- 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 (15) بنك، بالإضافة إلى قطاع الاتصالات والاعلام وتكنولوجيا المعلومات والتي بلغ عددها (15) شركة، ليصبح عدد الشركات الممثلة لمجتمع الدراسة (30) 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 (BIG4)، ومن ثم جودة التقارير المالية، مما يتيح الفرصة لإمكانية تشغيل النموذج المقترح لقياس الإفصاح عن المخاطر السيبرانية، من خلال تحليل المحتوى المعلوماتي للتقارير المالية والسنوية والمواقع الالكترونية. **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، وتكون خاضعة للتداول 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 .
✓ أن تتوافر التقارير المالية وتقرير مجلس الإدارة وتقارير الاستدامة للشركة بانتظام، والافصاح عنها من خلال موقع الشركة الإلكتروني على شبكة الانترنت، وأن تتوافر فيها بيانات كافية لحساب متغيرات الدراسة.

وقد أسفر تطبيق المعايير السابقة عن اختيار عدد (10) بنوك و (12) شركة تكون (22 شركة× 6 سنوات) (132) مشاهدة/سنة لتمثل عينة الدراسة، ويوضح الجدول التالي أسماء البنوك والشركات الممثلة في عينة الدراسة، وذلك كما يلى:

جدول رقم (4)
أسماء البنوك والشركات الممثلة في عينة الدراسة

م	القطاع	اسم الشركة	كود الترقيم الدولى	تاريخ القيد في البورصة	الحصة في رأس المال السوقي والقيمة السوقية 2023/10/25
1	قطاع البنوك (10 بنوك)	البنك التجاري الدولي- مصر	EGS60121C018	1995/02/02	%24.29
2		بنك الشركة المصرفية العربية الدولية (SAIB)	EGS60142C014	1980/11/29	
3		بنك أبو ظبي التجاري	EGS60111C019	1996/06/19	القيمة السوقية للقطاع
4		بنك التعمير والإسكان	EGS60301C016	1983/09/13	
5		بنك الكويت الوطني - مصر (NBKE)	EGS60171C013	1994/09/1	
6		بنك قناة السويس	EGS60231C015	1982/09/15	
7		بنك قطر الوطني الأهلي	EGS60081C014	1996/07/03	314,449,030,347
8		بنك كريدي أجريكول مصر	EGS60041C018	1996/07/03	
9		البنك المصري لتنمية الصادرات	EGS60241C014	1995/12/30	
10		البنك المصري الخليجي	EGS60182C010	1983/11/14	
1	قطاع الاتصالات والاعلام وتكنولوجيا المعلومات (12 شركة)	المصرية للأقمار الصناعية (نايل سات)	EGS48022C015	1998/12/09	%9.04
2		المصرية للاتصالات	EGS48031C016	1999/12/29	
3		فودافون مصر للاتصالات (VODE)	EGS48001C019	1998/05/26	
4		فوري لتكنولوجيا البنوك والمدفوعات الالكترونية	EGS745L1C014	2016/07/28	
5		المصريه لمدينة الانتاج الاعلامى	EGS78021C010	1999/09/26	
6		مصر جنوب افريقيا للاتصالات	EGS48271C018	2014/11/16	
7		المؤشر للبرمجيات ونشر المعلومات	EGS745W1C011	2010/02/01	
8		قناة السويس لتوطين التكنولوجيا (SCTS)	EGS740C1C010	2004/03/14	القيمة السوقية للقطاع
9		اي فاينانس للاستثمارات المالية والرقمية	EGS743O1C013	2005/02/01	
10		اوراسكوم للاستثمار القابضه للاتصالات والاعلام والتكنولوجيا	EGS693V1C014	2012/01/02	117,027,341,792
11		فرتيكا للصناعة والتجارة (VERT)	EGS74801C019	2013/04/30	
12		راية لخدمات مراكز الاتصالات	EGS74191C015	2015/02/11	
الإجمـالـي			22 شركة × 6 سنوات = 132 مشاهدة		

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

4/1- مصادر الحصول على البيانات: اعتمدت الدراسة التطبيقية **على أسلوب تحليل المحتوي الوصفى** في قياس مستوى الإفصاح 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.

5/1- طرق قياس متغيرات الدراسة: يمكن توضيح طرق قياس متغيرات الدراسة، كما يلى:

1/5/1- المتغير المستقل: الإفصاح عن المخاطر السيبرانية (CRD) : على الرغم من عدم وجود تقرير خاص أو شكل معين للإفصاح 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 والتقارير السنوية، 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 عن المخاطر السيبرانية بالشركات المقيدة فى البورصة يتكون من (53) بند **(ملحق)** يعتمد على مايلى:

- **إصدرات 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 2022. والدليل الإرشادي لـ (SEC, 2011; 2018) . وفي ضوء تكامل إطار COBIT.5، ومعايير الآيزو ISO 27001، وسلسلة NIST SP 800 . ومؤشر الإفصاح عن المخاطر السيبرانية لبورصة تورنتو (TSX) الكندية.
- **الاستراتيجية المصرية للأمن السيبراني (2017-2021)،** لمراعاة ظروف البيئة المصرية في المؤشر.
- **الموشرات الأخرى،** التى إستخدمتها الدراسات السابقة في قياس مستوى الإفصاح عن المخاطر السيبرانية (يعقوب وآخرون، 2022؛ Héroux and Forting, 2020; Heidenborg and Lappalainen, 2021; Eijkelenboom and Nieuwesteeg, 2021)

ويتكون المؤشر المقترح من **المحاور الخمس** التالية، وهي: (قنوات الاتصال الإلكترونية للشركة (8 بنود)، و المخاطر السيبرانية الفعلية والمحتملة (11 بند)، و لآثار المحتملة للمخاطر السيبرانية (6 بنود)، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (13 بند)، وأخيراً استراتيجيات تخفيف المخاطر السيبرانية (15 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 وذلك كما يلى:

- ✓ إعطاء متغير وهمى للبنود التي يحتويها المؤشر بحيث يتم إعطاء القيمة (1) إذا كانت الشركة تفصح عن البند وإعطاء القيمة (0) إذا كانت الشركة لا تفصح عن البند (البند غير موجود) .
- ✓ تجميع الدرجات لكل شركة ونسبتها إلى الحد الأقصى للبنود الواجب الإفصاح عنها وهى 53 بند، ومن ثم يمكن حساب مستوى الإفصاح عن المخاطر السيبرانية لكل شركة وذلك من خلال المعادلة التالية:

مستوى الإفصاح عن المخاطر السيبرانية وفقاً للمؤشر المقترح = (إجمالي بنود الإفصاح الفعلي من قبل الشركة/ إجمالي درجات بنود الإفصاح بالمؤشر (53 بند) ×100

2/5/1- المتغير التابع: (تكلفة رأس المال (WACC) :

توجد العديد من النماذج المقترحة لقياس تكلفة رأس المال من حق الملكية والديون في الفكر المحاسبي، حيث تختلف سمات ومخاطر كل مصدر منها (Havakhor et al., 2021, p. 16) . **واعتمد الباحث** على تكلفة المتوسط المرجح لقياس تكلفة رأس المالK، ويهدف إلى تقييم قدرة الشركة على استثمار أموالها (Bertomeu and Cheynel, 2016) . ويتم حسابه بقياس تكلفة كل عنصر من مكونات رأس المال على حده ثم ترجيح هذه التكلفة بنسبة العنصر في هيكل تمويل الشركة (Artiach and Clarkson, 2014) . **واعتمد الباحث على تكلفة المتوسط المرجح** لقياس تكلفة رأس المال (WACC)، استناداً على دراسة (Havakhor et al., 2021, p14)، والتي تناولت العلاقة بين الإفصاح عن استثمارات الأمن السيبراني وتكلفة رأس المال.

ويتم قياسه وفقاً للمعادلة الآتية (بريك،٢٠٢٠؛ الصاوي، 2022، ص73؛ Omran and Pointon, 2004; Ezat, 2019; Havakhor et al., 2021, p16; Kovner and Van Tassel, 2022, p1348; Dick-Nielsen et al., 2022, p2580; Rodríguez, 2023, p17; Rasheed, 2023, p21) :

$$\mathbf{WACC = CD \times \left[\frac{D}{V}\right] + CE\left[\frac{E}{V}\right]}$$

حيث أن: WACC: المتوسط المرجح لتكلفة رأس المال، وCD : تكلفة الديون، و (D) : اجمالي ديون الشركة، و$\left[\frac{D}{V}\right]$: نسبة القيمة الدفترية لديون الشركة (D) إلى إجمالي مكونات رأس المال (V)، و (CE) تكلفة حقوق الملكية، وE : إجمالي حقوق الملكية، و$\left[\frac{E}{V}\right]$نسبة القيمة الدفترية لقيمة حقوق الملكية (E) إلى إجمالي مكونات رأس المال (V)، وV= (E+D) .، **ولقياس تكلفة الديون:** يمكن الاعتماد علي معدل الفائدة المطلوبة في الأسواق المالية مقابل الاقتراض، وهذا المعدل عادة ما يُعلن عنه البنك المركزي كسعر محدد للفائدة مقابل تلك الأموال المقترضة، وسيعتمد الباحث في قياسها على دراسة (Bertomeu and Cheynel, 2016, p 226) وهي متوسط معدل الفائدة المدفوع مقسوماً على متوسط الديون (القيمة الدفترية لاجمالي الديون قصيرة وطويلة الأجل والسندات في بداية ونهاية الفترة/2) . **واعتمد الباحث في الدراسة التطبيقية علي هذا النموذج في تحديد تكلفة الديون، حيث يتميز بسهولة وبساطة استخدامه وتوافر بياناته في البيئة المصرية، واستناداً على دراسة كل من (Sheneman, 2017,**

p31; Harris et al., 2023, p198; Chatterjee et al., 2024, p37)، والتي تناولت العلاقة بين الإفصاح عن المخاطر السيبرانية وتكلفة الديون.

وتحدد تكلفة الاقتراض من خلال المعادلة التالية (مليجي، 2017، ص12؛ عازر، 2022، ص45؛ فرج وآخرون، 2022, ص80؛ Sheneman, 2017, p31; Ezat , 2019; Ayuningtyas and Harymawan, 2021, p134; Le et al., 2021; Shad et al., 2022,p88; Alia and AbuSarees, 2023, p4; Khelil, (2023, p12; :

$$\mathbf{CDit} = \frac{\mathbf{ICit}}{\mathbf{TDit}} \times (\mathbf{1} - \mathbf{TR})$$

حيث أن: (CD_{it}) تكلفة الديون للشركة i في السنةt، و **(IC_{it})** إجمالي مصروفات الفائدة للشركة **i** في السنة**t**، وهي التكلفة التي تتحملها الشركة مقابل اقتراضها، وتمثل الفوائد المدينة، أو الفوائد التمويلية أو مصروفات الفوائد، ويمكن الحصول عليها من **قائمة الدخل**، و **(TD_{it})** متوسط إجمالي الديون للشركة **(I)** في السنة**t**، ويتم حسابه عن طريق إيجاد الوسط الحسابي لإجمالي الديون في السنة **(t)** وإجمالي الديون في السنة **(t- 1)**، **أي (رصيد الديون قصيرة وطويلة الأجل أول الفترة+ رصيد الديون قصيرة وطويلة الأجل أخر الفترة) /2 .** ويمكن الحصول عليها من **الميزانية (قائمة المركز المالي) .** وعند تحديد إجمالي الديون للبنوك، يتم إضافة المبلغ الإجمالي للودائع للحصول على هذا العنصر المهم للرافعة المالية للبنك(Kovner and Van Tassel, 2022, p1348 .) و **(TR)** معدل (سعر) الضريبة الفعلي على الدخل (مصروف الضريبة الحالية ÷ صافي الربح قبل الضرائب)، ويمكن الحصول عليها من **قائمة الدخل، وهناك بعض الشركات تفصح عنه في الايضاحات المتممة للقوائم المالية.**

ولقياس تكلفة حقوق الملكية: اعتمد الباحث على نموذج (Omran and Pointon, 2004)، حيث يعتمد علي المعلومات المحاسبية الفعلية في القوائم المالية، وتطبيقه في الأسواق الناشئة وبصفة خاصة علي منشآت الأعمال المصرية، وتقوم فكرة هذا النموذج على أنه يمكن تقدير تكلفة حقوق الملكية بناءً على مقلوب نسبة السعر لربحية السهم، وطبقاً لهذا النموذج تتحدد تكلفة حقوق الملكية على النحو التالي (مليجي، 2017، ص12؛ الزهيري، وآخرون، 2022، ص192-193؛ عازر، 2022، ص44؛ الشريف, 2023، ص561؛ Omran and Pointon, 2004, p257; Alia and AbuSarees, 2023, p4) :

$$CE = \frac{1}{PE\ ratio - (eo - do)/eo}$$

حيث أن: CE: تكلفة حقوق الملكية (الأسهم العادية والممتازة والأرباح المحتجزة)، و$PE\ ratio$: مضاعف ربحية السهم (نسبة سعر السهم السوقي في نهاية السنة إلى ربحية السهم)، وeo : نصيب السهم من الأرباح المحققة في العام الحالي (صافي الربح المحاسبي بعد الضريبة/ متوسط عدد الأسهم المصدرة والمتداولة)، وdo : نصيب السهم من الأرباح الموزعة في العام الحالي.

واعتمد الباحث علي هذا النموذج في تحديد تكلفة حقوق الملكية، حيث يتميز بسهولة استخدامه، فضلاً عن اعتماده على متغيرات محاسبية يمكن توفيرها من خلال القوائم المالية، الأمر الذي يجعل هناك إمكانية لتطبيقه على المنشآت العاملة في البيئة المصرية، وافتقار بيئة الأعمال المصرية إلى بعض البيانات التي تحتاجها النماذج الأخرى، واستناداً على دراسة كل من (Ashraf and Sunder , 2023, p17-18; Elmawazini et al., 2023, p3)، والتي تناولت العلاقة بين الإفصاح عن خرق البيانات وتكلفة حقوق الملكية.

3/5/1- المتغيرات الرقابـــــية (CONTROL VARIABLE) : تشـمل المتغيرات الرقابية بعض العوامل المؤثرة على المتغيرات التابعة (قد تكون ذات تأثير محتمل على تكلفة رأس المال المقترض والمملوك)، ولكنها لا تدخل في نطاق الدراسـة محل البحث، وتم إضـافتها من أجل ضـبط العلاقة بين المتغير المسـتقل والمتغير التابع، ومن أهم هذه المتغيرات ما يلى:

- **حجم الشركة (SIZE) :** تعبر 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 (Kamiya et al., 2021, 727). **ويقاس حجم الشركة باللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام** (McShane and Nguyen, 2020, p580; Firoozi and Mohsni, 2023, p16).

- **درجة الرافعة المالية (Leverage) :** 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. (Kamiya et al., 2021, p724; Gatzert and Schubert, 2022, p739). **ويتم قياس درجة الرفع المالي للشركة من خلال قسمة إجمالي الالتزامات على إجمالي الأصول**. (McShane and Nguyen, 2020, p580;Firoozi and Mohsni, 2023, p16) .
- **ربحية الشركة (ROA)** : ويعبر عنه بمعدل العائد على الأصول والذى يدل على جودة الأداء المالى للشركة ويوثر على سمعة وأداء الشركة في السوق، **ويحسب (ROA) من خلال صافي ربح العام قبل الضرائب مقسوماً على إجمالي الأصول** (Zhou et al., 2023, p113; Firoozi and Mohsni, 2023, p16) .
- **نسبة الأصول غير الملموسة (INTAN) :** قد تؤدي الحوادث السيبرانية أيضاً إلى تقلص التدفقات النقدية المستقبلية، مما يتطلب النظر في انخفاض قيمة بعض الأصول بما في ذلك الشهرة والأصول غير الملموسة كالعلامة التجارية وبراءة الاختراع والبرامج المرسملة، أو غيرها من الأصول طويلة الأجل المرتبطة بالأجهزة أو البرامج(FASB ASC450-20, 2020) . **وتم قياس نسبة الأصول غير الملموسة بقسمة إجمالي قيمة الأصول غير الملموسة على إجمالي الأصول خلال الفترة**، وذلك **قياساً على دراسة** كل من (Avery, 2021, p501; Firoozi and Mohsni, 2023, p16; Harris et al., 2023, p198) . **ويمكن للباحث توضيح طريقة قياس متغيرات الدراسة من خلال الجدول التالي:**

جدول رقم (5)
التعريف الإجرائي بمتغيرات الدراسة

المتغيرات	الرمز	طريقة القياس	نوع المتغير	مصدر الحصول على البيانات
أولا: المتغير التابع : (تكلفة رأس المال المقترض والمملوكWACC)				
المتوسط المرجح لتكلفة رأس المال	WACC	$WACC = CD \times \left[\frac{D}{V}\right] + CE\left[\frac{E}{V}\right]$ حيث أن: WACC= المتوسط المرجح لتكلفة رأس المال، E/V = نسبة حقوق الملكية (E) إلى إجمالي مكونات رأس المال (V)، (E + D) = V، D/V= نسبة قيمة ديون الشركة (D) إلى إجمالي مكونات رأس المال (V)، CE = تكلفة حق الملكية ويمكن قياسها وفقا لنموذج (Omran and Pointon, 2004) حيث يعتمد علي المعلومات المحاسبية الفعلية المتوفرة في القوائم المالية، وتطبيقه في الأسواق الناشئة وبصفة خاصة علي منشآت الأعمال المصرية،CD = تكلفة الإقتراض، وسيعتمد الباحث في قياسها على دراسة (Bertomeu and Cheynel, 2016) وهي متوسط معدل الفائدة المدفوع مقسوماً على متوسط الديون قصيرة و وطويلة الأجل	تابع	التقارير المالية للشركات
ثانيا: المتغير المستقل : (الإفصاح عن المخاطر السيبرانية)				
الإفصاح عن المخاطر السيبرانية	CRD	قام الباحث بإتباع نفس نهج العديد من الدراسات السابقة بتكوين مؤشر لقياس مستوى الإفصاح عن المخاطر السيبرانية بالشركات المقيدة فى البورصة يتكون من (53) بند ويتكون المؤشر المقترح من المحاور الخمس التالية، وهي: (قنوات الاتصال الإلكترونية للشركة (8 بنود)، والمخاطر السيبرانية الفعلية والمحتملة (11 بند)، و الآثار المحتملة للمخاطر السيبرانية (6 بنود)، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (13 بند)، وأخيراً تخفيف المخاطر السيبرانية (15 بند) .	مستقل	التقارير المالية وغير المالية للشركة والمواقع الإلكترونية للشركات
ثالثاً: المتغيرات الحاكمة : (المتغيرات الرقابية)				
حجم الشركة	SIZE	يقاس باللوغاريتم الطبيعي لإجمالي 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 .		
نسبة الأصول غير الملموسة	INTAN	يقاس بنسبة إجمالي الأصول غير الملموسة على إجمالي الأصول .		

المصدر: الباحث، إعتماداً على الدراسات ذات الصلة.

6/1- 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 عن المخاطر السيبرانية، ينشأ نموذج

أساسي للبحث يهدف إلى قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك في ضوء العوامل الرقابية، ويغطى هذا النموذج الفرض الثالث للدراسة، ويمكن التعبير عن النموذج بالمعادلة الكمية التالية:

$$WACC = \beta_0 + \beta_1 (CRD) + \beta_2 (SIZE) + \beta_3 (ROA) + \beta_4 (LEV) + \beta_5 (INTAN) + \varepsilon_{it}$$

حيث **(WACC)** : المتغير التابع وهو تكلفة رأس المال المقترض والمملوك، **(CRD)** : المتغير المستقل وهو الإفصاح عن المخاطر السيبرانية، **(SIZE)** هو حجم الشركة، **(ROA)** ربحية الشركة، **(LEV)** درجة الرفع المالى للشركة، **(INTAN)** نسبة الأصول غير الملموسة، والباحث إفترض مبدئيا وجود علاقة إيجابية بين جميع المتغيرات المستقلة والمتغيرات التابعة.

2- تحليل نتائج الدراسة واختبار الفروض: قام الباحث بتطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية [Statistical Package for Social Science (SPSS)] (**الإصدار (25) فى تحليل البيانات إحصائياً**) وقد تطلبت طبيعة البيانات تحديد الأساليب الإحصائية اللازمة والملائمة، والتي تتمثل فيما يلي: (سليمان، 2007، 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 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:

1/2- اختبار صلاحية البيانات للتحليل الإحصائي: ويتم ذلك من خلال القيام بما يلي:

1/1/2- 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 ما بين اختبارات الإحصاء المعلمى واختبارات الإحصاء اللامعلمى، والجدول التالي يوضح قيم الاختبارات ومستوى المعنوية لكل متغير أمام كل اختبار:

جدول رقم (6)
التوزيع الطبيعي لمتغيرات الدراسة

Variables		Kolmogorov-Smirnov Statistic		Shapiro-Wilk Statistic	
		Value	Sig.	Value	Sig.
الإفصاح عن المخاطر السيبرانية	CRD	.164	.000	.890	.000
تكلفة رأس المال المقترض	CD	.191	.000	.800	.000
تكلفة رأس المال المملوك	CE	.187	.000	.697	.000
تكلفة رأس المال	WACC	.189	.000	.706	.000
حجم الشركة	SIZE	.133	.000	.947	.000
ربحية الشركة	ROA	.276	.000	.634	.000
درجة الرفع المالى	LEV	.244	.000	.789	.000
نسبة الأصول غير الملموسة	INTAN	.317	.000	.521	.000

المصدر: نتائج التحليل الاحصائي.

ويتضح من الجدول السابق أن قيمة مستوى المعنوية (Sig.) لاختبار (Kolmogorov-Smirnov)، ماعدا درجة الرفع المالي، واختبار (Shapiro-Wilk) أقل من (0,05) لجميع المتغيرات، وبناءً على ذلك فإن البيانات الخاصة بمتغيرات الدراسة لا تتبع التوزيع الطبيعي، وبناءً على النتيجة السابقة فإن البيانات الخاصة بمتغيرات الدراسة لا تتبع 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، 2012)، وفى ضوء ماسبق يلتزم الباحث عند إختبار الفروق المرتبطة بالمتغيرات التى لاتتبع بياناتها التوزيع الطبيعى إستخدام الإختبارات اللامعلمية.

1/1/2- اختبـــــار 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: **جدول رقم (7)**

نتائج اختبار (M. C. Test) لنماذج الدراسة

المتغيرات المستقلة فى نموذج الدراسة (مستقلة ورقابية)		نتائـــــج إختبـار التداخـل الخطى Collinearity Test المتغيرات التابعة					
		CD		CE		WACC	
المتغير المستقل		Tolerance	VIF	Tolerance	VIF	Tolerance	VIF
	CRD	0.832	1.202	.898	1.114	0.956	1.046
متغيرات رقابية	SIZE	0.799	1.252	.811	1.234	0.639	1.566
	ROA	0.873	1.145	.835	1.197	0.867	1.154
	LEV	0.708	1.413	.893	1.120	0.649	1.542
	INTAN	0.986	1.014	.986	1.014	0.716	1.396

المصدر: نتائج التحليل الاحصائي.

يتضح للباحث من الجدول السابق أن قيم (VIF) لجميع المتغيرات المستقلة ومتغيرات الرقابة في نموذج الدراسة أقل من (10)، 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.

3- 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:

جدول رقم (8)

نتائج اختبار الارتباط الذاتي (Durbin Watson Test)

المتغيرات التابعة	نتائج اختبار الارتباط الذاتي Durbin Watson Test		
	CD	CE	WACC
قيمة (D-W)	1.592	2.161	1.867

المصدر: نتائج التحليل الاحصائي.

ويتضح للباحث من الجدول السابق أن قيم D-W) المحسوبة تقترب من المدى المثالي وهو الذي يقع بين (1.5،2.5)، وفقا لجدول (Durbin Watson Test) عند مستوى معنوية (0.05) 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، وبالتالي قوة نماذج الدراسة وزيادة قدرتها التفسيرية، ومن ثم صلاحية البيانات للتحليل الإحصائي.

3/1/2- التحليل الوصـفي لمتغيرات الدراسـة: يظهر الجدول التالى نتائج توصـيف متغيرات الدراسـة وذلك على مدار سنوات الدراسة وعلى مستوى كل المشاهدات **(panel data)**، وذلك كما يلى:

جدول رقم (9)
الإحصاء الوصفي لمتغيرات الدراسة

النوع	متغيرات الدراسة	الرمز	المتوسط الحسابي		الانحراف المعياري	أقل قيمة	أقصى قيمة	التباين
المتغير المستقل	الإفصاح عن المخاطر السيبرانية	CRD	عدد	32.62	14.111	8	52	199.107
			نسبة	0.615	0.2662	0.1509	0.9811	0.071
المتغيرات التابعة	تكلفة الديون	CD	0.067734		0.07290	0.0013	0.7158	0.0053
	تكلفة حقوق الملكية	CE	0.2021		0.1693	0.0054	0.8820	0.029
	تكلفة رأس المال	WACC	0.09853		0.0886	0.0095	0.74439	0.080
المتغيرات الرقابية	حجم الشركة	Size	20.0378		3.4586	14.3566	26.8903	11.962
	ربحية الشركة	ROA	0.05105		0.06679	0.0032-	0.3217	0.004
	درجة الرافعة المالية	LEV	0.4595		0.3799	0.0018	0.9231	0.144
	نسبة الأصول غير الملموسة	INTAN	0.06883		0.1443	0.001	0.7167	0.021

المصدر: نتائج التحليل الاحصائي.

ويلاحظ من الجدول السابق، أن شركات العينة تفصح عن المخاطر السيبرانية بمتوسط عام بلغ (32.62) بند من إجمالى (53) بند الممثلين للمؤشر المقترح، بنسبة إفصاح بلغت (62%) تقريباً، وأن هناك تحسن ملحوظ في مستوى الإفصاح عن المخاطر السيبرانية لعينة الدراسة خلال السنوات (2017: 2022)، ويوضح الإحصاء الوصفى لمتغير الافصاح عن المخاطر السيبرانية، أن الحد الأقصى للإفصاح بلغ (98.11%) وتحقق ذلك عام 2022، كما أفصحت شركات العينة بأقل قيمة للإفصاح عند (15.1%) وذلك في عام 2017.

و**تتفق** هذه النتائج مع دراسة (Héroux and Fortin, 2020)، والتي توصلت أن مستويات الإفصاح عن المخاطر السيبرانية منخفض. **ونتائج دراسة (Godoy, 2021)**، والتي توصلت إلى أن69٪ من الشركات تفصح عن قضايا الأمن السيبراني الخاص بهم في قسم (A1) . **وكذلك اتفاقها مع نتائج** دراسة **(Ereddia, 2023)، والتي توصلت إلى** أن أكثر من 36%من الشركات لا تقدم أي معلومات حول دور مجلس الإدارة في الإشراف على المخاطر السيبرانية. وذلك على **عكس** دراسة (Eijkelenboom and Nieuwesteeg, 2021)، والتي توصلت إلى أنه على الرغم من عدم وجود التزام قانوني للإفصاح عن الأمن السيبراني، فإن 87 ٪ 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 عن المخاطر السيبرانية، والتي لاحظها الباحث عند إستيفاء بنود المؤشر المقترح لقياس مستوى الإفصاح 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 –باستثناء- شركتين وبنك من عينة الدراسة) .
- ✓ عدم توافر الضمانات والتأكيدات المستقلة حول معلومات المخاطر السيبرانية المفصح عنها.

وبالنسبة لتكلفة الديون (رأس المال المقترض)، بلغ المتوسط الحسابي (0.06773) بانحراف معياري (0.07290)، ويعني ذلك انخفاض تكلفة الديون خلال فترة الدراسة، وأشارت النتائج إلى أن إلى أن أقل قيمة وأقصى قيمة لتكلفة رأس المال المقترض (الديون) بالشركات في السوق بلغت (0.0013)، و (0.7158)، بينما **بلغ** المتوسط الحسابي **لتكلفة حقوق الملكية (رأس المال المملوك)** (0.2021) بانحراف معياري (0.1693) خلال فترة الدراسة، وأشارت النتائج إلى أن إلى أن أقل قيمة وأقصى قيمة لتكلفة رأس المال الملوك (حقوق الملكية) بالشركات والبنوك محل الدراسة في السوق بلغت (0.0054)، و (0.8820) .

وأشارت نتائج التحليل الوصفي بالنسبة لتكلفة رأس المال، بلغ المتوسط الحسابي لتكلفة رأس المال (0.09853) بانحراف معياري (0.0886)، ويعني ذلك انخفاض تكلفة رأس المال خلال فترة الدراسة، وأشارت النتائج إلى أن أقل قيمة وأقصى قيمة لتكلفة رأس المال (WACC) بالشركات في السوق بلغت (0.0095)، و (0.7744)، **ويعزى الباحث** هذا الارتفاع في بعض الشركات محل الدراسة إلى احتمالية تأثر تكلفة رأس المال بأحداث التضخم المحيطة وارتفاع الصراعات السياسية وأسعار الفائدة نتيجة الأحداث العالمية الناتجة عن الأزمة الروسية الأوكرانية والعدوان الاسرائيلي الغاشم، وما أحدثته من أثار سلبية على أسواق المال.

وبالنسبة للمتغيرات الرقابية توضح النتائج، أن متوسط اللوغاريتم الطبيعي لإجمالي أصول شركات العينة والدال على **حجم الشركة** قيمة (20.04) بانحراف معياري (3.4586)، وتؤكد النتائج على ارتفاع حجم الشركات من عام 2017 حتى عام 2022، وبالنسبة **للأداء المالي** للشركات والذى يعبر عنه بربحية الشركة بدلالة معدل العائد على الأصول، توضح النتائج أن ربحية شركات العينة جاء بمتوسط عائد بلغ (0.051%)، وأن هناك تذبذب في ربحية شركات العينة، وبلغت أعلى نسبة وأقل نسبة ربحية (0.3217)، و (-0.0032) خلال فترة الدراسة. كما بلغت **الرافعة المالية**، والتي توضح مدي اعتماد الشركة على الديون في تمويل أصولها، فتشير النتائج إلى أن متوسط معدل الرافعة المالية بلغ (0.4595) بانحراف معياري (0.3799)، وهو ما يعكس إمكانية قدرة عينة الدراسة في الحصول على التمويل اللازم، وتدل على مديونية الشركة كأحد العوامل التي تؤثر على تكلفة رأس المال وقيمة المنشأة، ويلاحظ من النتائج زيادة هذه النسبة من سنة لأخرى حيث تراوحت بين (0.0018)، (0.9231)، **وفيما يتعلق بمتوسط اقتناء الأصول غير الملموسة**، والذى بلغ (0.06883)، وقد تكون هذه النسبة هامة عند قياس العلاقة بين الإفصاح عن المخاطر السيبرانية وقيمة المنشأة، وتؤكد النتائج على ارتفاع نسبة الأصول غير الملموسة في الشركات محل الدراسة، حيث تراوحت بين (0.0001)، (0.7167)، وتوفر هذه النتيجة التأكيد على أن جميع شركات العينة محل الدراسة تحتفظ بأصول غير ملموسة، وهذه النسبة آخذة في الازدياد مع مرور الزمن وتحول الشركات رقمياً، وهو ما يتوافق مع تحول الدولة المصرية ورؤيتها 2030، للشركات والبنوك نحو الشمول المالي ورقمنة العمليات، وهذا يتطلب أن نأخذ المخاطر السيبرانية بمحمل الجد وتحليل أثارها الحالية والمحتملة على أداء الشركات، وتحديد نطاق تأثيرها على كل من القوائم والتقارير السنوية وأسعار الأسهم وتكلفة رأس المال والأداء المالي المستدام، بالإضافة إلى تأثيرها على مدى استمرارية المنشأة، وانعكاسها على ترشيد قرارات المستثمرين. وفى إطار توصيف متغيرات الدراسة، يوضح الجدول التالي الإحصاء الوصفي لمتغيرات الدراسة على مستوى البنوك والشركات الممثلة لقطاعات العينة وذلك كما يلى:

جدول رقم (10)
الإحصاء الوصفى لمتغيرات الدراسة حسب نوع القطاع

القطاع	الإحصائيات الوصفية	نسبة الإفصاح عن المخاطر السيبرانية		تكلفة الديون	تكلفة حقوق الملكية	المتوسط المرجح لتكلفة رأس المال	حجم الشركة	ربحية الشركة	درجة الرفع المالى	نسبة الأصول غير الملموسة
		CRD								
		عدد	نسبة	CD	CE	WACC	Size	ROA	LEV	INTAN
قطاع البنوك (60) مشاهدة	المتوسط	35.6	0.672	0.0491	0.2953	0.0785	22.121	0.0266	0.8501	0.00104
	الإنحراف المعيارى	13.177	0.249	0.0242	0.1635	0.0384	3.273	0.0226	0.1072	0.001
	أقصى قيمة	52	0.981	0.1926	0.8820	0.2537	26.890	0.102	0.9231	0.0051
	أقل قيمة	11	0.208	0.0226	0.0871	0.031	17.503	0.032-	0.3158	0.0001
	التباين	173.73	0.062	0.0006	0.0267	0.0015	10.710	0.001	0.011	0.0000
شركات اتصالات واعلام وتكنولوجيا المعلومات (72)	المتوسط	30.14	0.569	0.0833	0.1244	0.1153	18.302	0.0714	0.1339	0.12533
	الإنحراف المعيارى	14.468	0.273	0.0937	0.1311	0.1123	2.539	0.0830	0.1424	0.1769
	أقصى قيمة	50	0.943	0.7158	0.8421	0.7444	22.476	0.3217	0.5227	0.7167

القطاع	الإحصائيات الوصفية	نسبة الإفصاح عن المخاطر السيبرانية		تكلفة الديون	تكلفة حقوق الملكية	المتوسط المرجح لتكلفة رأس المال	حجم الشركة	ربحية الشركة	درجة الرفع المالى	نسبة الأصول غير الملموسة
		CRD								
		عدد	نسبة	CD	CE	WACC	Size	ROA	LEV	INTAN
مشاهدة	أقل قيمة	8	0.151	0.0013	0.0172	0.0095	14.357	0.0028	0.0018	0.0002
	التباين	209.33	0.075	0.0088	0.0213	0.0126	6.4486	0.007	0.0203	0.031

المصدر: نتائج التحليل الاحصائي.

ويلاحظ من الجدول السابق أن قطاع البنوك يفصح عن المخاطر السيبرانية بمتوسط (67.2%)، ومتوسط تكلفة الديون للبنوك بلغت (0.491)، كما بلغ متوسط تكلفة حقوق الملكية (29.53)، وتكلفة رأس المال بلغت (7.85)، كما اللوغاريتم الطبيعى لإجمالى الأصول والدال على حجم القطاع (22.121)، بمتوسط ربحية بلغت (0.0266)، ودرجة رفع مالى بلغت في المتوسط (0.8501)، كما بلغت نسبة الأصول غير الملموسة إلى إجمالي الأصول في قطاع البنوك (0.00104)، من إجمالي قيمة الأصول، في مقابل أن **شركات الاتصالات وتكنولوجيا المعلومات والاعلام** تفصح عن المخاطر السيبرانية بمتوسط (30.14%)، ومتوسط تكلفة الديون للبنوك بلغت (0.0833)، كما بلغ متوسط تكلفة حقوق الملكية (12.44)، وتكلفة رأس المال بلغت (11.53)، كما بلغ متوسط اللوغاريتم الطبيعى لإجمالى الأصول والدال على حجم القطاع (18.302)، بمتوسط ربحية بلغت (0.0714)، ودرجة رفع مالى بلغت في المتوسط (0.1339)، كما بلغت نسبة الأصول غير الملموسة إلى إجمالي الأصول في قطاع الاتصالات وتكنولوجيا المعلومات والاعلام (0.12533)، من إجمالي قيمة الأصول.

3- 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:

1/3- اختبار الفـــــرض الأول: حيث ينص الفرض الأول على: يوجد تفاوت في الإفصاح 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 ليتناسب مع متغير الإفصاح عن المخاطر السيبرانية والذي لاتتتبع بياناته التوزيع الطبيعى، وذلك كما يلى:

جدول رقم (11)

التمايز في مستوى الإفصاح عن المخاطر السيبرانية بين قطاع البنوك وقطاع الاتصالات وتكنولوجيا المعلومات

القطاع	الإحصائيات الوصفية	المجموعات المكونة للمؤشر المقترح لقياس مستوى الإفصاح عن المخاطر السيبرانية					مستوى الإفصاح عن المخاطر السيبرانية
		قنوات الاتصال الإلكترونية للشركة (8) بنود	المخاطر السيبرانية الفعلية والمحتملة (11) بند	الآثار المحتملة للمخاطر السيبرانية (6) بنود	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (13) بند	تخفيف المخاطر السيبرانية (15) بند	
قطاع البنوك (60 مشاهدة)	المتوسط	7.55	6.98	2.62	7.87	10.58	35.6
	الإنحراف المعيارى	0.982	3.685	1.485	4.304	3.954	13.177
	أقصى قيمة	8	11	6	13	15	52
	أقل قيمة	4	1	1	0	1	11

القطاع	الإحصائيات الوصفية	المجموعات المكونة للمؤشر المقترح لقياس مستوى الإفصاح عن المخاطر السيبرانية					مستوى الإفصاح عن المخاطر السيبرانية
		قنوات الاتصال الإلكترونية للشركة (8) بنود	المخاطر السيبرانية الفعلية والمحتملة (11) بند	الآثار المحتملة للمخاطر السيبرانية (6) بنود	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (13) بند	تخفيف المخاطر السيبرانية (15) بند	
	متوسط الرتب	69.76	75.82	77.50	73.62	71.55	76.01
شركات اتصالات واعلام وتكنولوجيا المعلومات (72 مشاهدة)	المتوسط	7.06	5.49	1.85	6.37	9.43	30.14
	الإنحراف المعيارى	1.884	4.025	1.274	4.874	4.553	14.468
	أقصى قيمة	8	11	5	13	15	50
	أقل قيمة	2	0	0	0	0	8
	متوسط الرتب	63.78	58.74	57.33	60.57	62.29	58.58
Mann-Whitney Test	Mann-Whitney U	1964.500	1601.000	1500.00	1733.000	1857.000	1589.500
	Asymp. Sig. (2-tailed)	0.240	0.010	0.002	0.047	0.164	0.009

المصدر: نتائج التحليل الاحصائي.

- يتضح من الجدول السابق أن مستوى المعنوية لاختبار (Mann-Whitney Test) قيمة (0.009) وهو أقل من (0.05) 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.
- وتوجد فروق ذات دلالة إحصائية بشأن المخاطر السيبرانية الفعلية والمحتملة، والآثار المحتملة للمخاطر السيبرانية، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة حيث بلغ مستوى المعنوية (0.010)، و (0.002)، و (.047) على التوالي، ولا توجد فروق بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات والاعلام بشأن الإفصاح عن قنوات الاتصال الإلكترونية، وتخفيف المخاطر السيبرانية، حيث بلغ مستوى المعنوية (0.240)، و (0.164) على التوالي.
- ويتضح من الجدول السابق، أن قطاع البنوك يفصح عن المخاطر السيبرانية بمتوسط (67.2%)، في مقابل أن شركات الاتصالات وتكنولوجيا المعلومات والاعلام تفصح عن المخاطر السيبرانية بمتوسط (56.9%)، وذلك خلال فترة الدراسة من (2017- 2022) .

وتتفق 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. **وتتفق مع نتائج دراسة (Duvenhage et al., 2022)، والتي توصلت إلى وجود** تمايز في الاختلاف بين مستويات الإفصاح عن المخاطر السيبرانية لكل قطاع ودولة. وكذلك **توصلت دراسة (يعقوب وآخرون, 2022)** إلى وجود اختلافات في افصاح عينة الدراسة وفق المؤشر المقترح للإفصاح عن المخاطر السيبرانية. 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 ونسبة الأصول غير الملموسة، بالإضافة إلى عدم وجود إطار موحد تلتزم به الشركات عند الإفصاح عن المخاطر السيبرانية أو حتى تسترشد به. **ويلاحظ من الجدول التالي** مدى الاختلاف بين شركات العينة وفقاً لاختلاف السنوات، وذلك من خلال مقارنة المتوسطات خلال فترة

الدراسة على مستوى مجموعات المؤشر المقترح لقياس تطور مستوى الإفصاح عن المخاطر السيبرانية، بالإضافة إلى تحليل نتائج إختبار Friedman Test لقياس التباين بين أكثر من عينتين مرتبطتين (السنوات)، وهو أحد الإختبارات اللامعلمية ليتناسب مع متغير الإفصاح عن المخاطر السيبرانية والذي لا تتتبع بياناته التوزيع الطبيعى، وذلك من خلال الجدول التالي رقم (13) كما يلى:

جدول رقم (12)
تطور مستوى الإفصاح عن المخاطر السيبرانية خلال فترة الدراسة (2017- 2022)

مستوى الافصاح عن المخاطر السيبرانية	الاحصاءات الوصفية	قنوات الاتصال الإلكترونية للشركة (8) بنود	المخاطر السيبرانية الفعلية والمحتملة (11) بند	الآثار المحتملة للمخاطر السيبرانية (6) بنود	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (13) بند	تخفيف المخاطر السيبرانية (15) بند	مستوى الإفصاح عن المخاطر السيبرانية
الفترة (2017-2022)	المتوسط	7.25	6.17	2.20	7.05	9.95	32.62
	الانحراف المعياري	1.560	3.931	1.422	4.666	4.314	14.111
	اقل قيمة	2	0	0	0	0	8
	أقصى قيمة	8	11	6	13	15	52
	Mean Rank	3.24	2.75	1.34	3.14	4.53	6
	N	132					
Friedman Test	Chi-Square	491.131					
	df	5					
	Asymp. Sig.	0.000					

المصدر: نتائج التحليل الاحصائي.

ويتضح من الجدول السابق أن قيمة (Chi-Square) بلغت (491.131)، وذلك بمستوى معنوية اختبار (0.000) وهو أقل من (0.05) للتباين حول مستوى الإفصاح عن المخاطر السيبرانية وفقاً لاختلاف السنوات، ويدل ذلك على وجود فروق معنوية بين شركات عينة الدراسة بشأن مستوى الافصاح عن المخاطر السيبرانية، وفقاً لاختلاف السنوات، وفى ضوء النتيجة السابقة ووفقا لمتوسط السنوات، يعد عام 2022هو الأعلى في مستوى افصاح شركات العينة عن المخاطر السيبرانية، ثم عام 2020، وأقلها افصاحاً عام 2017، وذلك بانحراف معياري على المستوى الاجمالي لبنود المؤشر المقترح للإفصاح عن المخاطر السيبرانية (14.111). **وتتفق هذه النتائج** مع دراسة (Chen et al., 2022)، والتي توصلت إلى أن كل من المنشآت المخترقة وغير المخترقة تزيد في المتوسط من مقدار الإفصاح عن عوامل المخاطر السيبرانية. ونتائج دراسة (Firoozi and Mohsni, 2023)، والتي توصلت إلى أن هناك زيادة كبيرة في الافصاح عن الأمن السيبراني بعد أن أصدر مسؤولو الأوراق المالية الكنديون إرشادات للإفصاح عن الأمن السيبراني، وهناك اختلافات كبيرة في الافصاح عن الأمن السيبراني بناءً على الصناعة والحجم، وهناك تحسناً في جميع فئات الافصاح بمرور الوقت.

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

2/3- تحليل نتائج اختبار الفرض الثانى، حيث ينص الفرض: يوجد ارتباط معنوى بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض والمملوك، ويتم اختبار هذه الفرض من خلال إعداد مصفوفة الارتباط لمتغيرات الفرض (الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض والمملوك والمتغيرات الرقابية) وذلك كما يلي:

جدول رقم (13)
نتائج تحليل مصفوفة الارتباط لمتغيرات الفرض الثانى

نوع المتغير	متغيرات الفرض	تكلفة رأس المال المقترض (CD)	تكلفة رأس المال المملوك (CE)	المتوسط المرجح لتكلفة رأس المال (WACC)	الإفصاح عن المخاطر السيبرانية (CRD)	حجم الشركة (Siz)	ربحية الشركة (ROA)	درجة الرفع المالى (LEV)	نسبة الأصول غير الملموسة INTAN) (
المتغيرات التابعة	تكلفة رأس المال المقترض (CD)	1							
	تكلفة رأس المال المملوك (CE)	*0.193	1						
		0.027							
	المتوسط المرجح لتكلفة رأس المال (WACC)	**0.353	**0.724	1					
		0.000	0.000						
المتغيرات المستقلة	الإفصاح عن المخاطر السيبرانية (CRD)	**0.564-	**0.380-	**0.487-	1				
		0.000	0.000	0.000					
المتغيرات الرقابية	حجم الشركة (Size)	**0.339-	0.11	*0.214-	*0.203	1			
		0.000	0.208	0.014	0.02				
	ربحية الشركة (ROA)	0.079-	0.036	0.089	0.028-	*0.202	1		
		0.369	0.678	0.308	0.748	0.02			
	درجة الرفع المالى (LEV)	**0.359	0.026-	**0.266	**0.381-	**0.350-	*0.192-	1	
		0.000	0.770	0.002	0.000	0.000	0.028		
	نسبة الأصول غير الملموسة (INTAN)	0.061-	0.103	0.080	*0.173	0.024	0.012-	0.021-	1
		0.488	0.24	0.364	0.048	0.789	0.895	0.814	

المصدر: نتائج التحليل الاحصائي.

**** تشير إلى معنوية معامل الارتباط عند مستوى معنوية 0.01 * تشير إلى معنوية معامل الارتباط عند مستوى معنوية 0.05**

ومن الجدول السابق يتضح للباحث النتائج الأتية:

- **وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض (تكلفة الديون)**، حيث أن معامل الارتباط سلبي بقيمة (-0.564) ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى **انخفاض تكلفة رأس المال المقترض (تكلفة الديون)** للشركة، **مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة ارتباط معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض (تكلفة الديون) .** وتتفق هذه النتائج مع دراسة (Havakhor et al., 2021, p4)، والتي توصلت إلى أنه يمكن أن يؤدي الإفصاح عن الأمن السيبراني إلى تقليل تكلفة رأس المال، من خلال تقليل عدم تناسق المعلومات حول قدرة الشركة على التعامل مع المخاطر السيبرانية، وبالتالي يجب أن تقلل هذه الإفصاحات من العوائد التي يفرضها المستثمرون على الشركة مقابل رأس المال الذي تقترضه. ولقد توصلت دراسة (Harris et al., 2023, p208) أنه مع **انخفاض** جودة إفصاح الشركات عن المخاطر السيبرانية في تقارير (K-10)، **تزداد تكلفة الديون** على هذه الشركات. على **عكس** دراسة (Vincent and Trussel, 2019, p495) التي توصلت إلى أن الإفصاح عن المخاطر السيبرانية لا تؤثر بشكل جوهري على مستوى تكلفة تمويل الديون. وفيما يتعلق **بمردود ادارة المخاطر السيبرانية**. فقد أشار (Havakhor et al., 2021) إلي أن الافصاح عن إدارة المخاطر السيبرانية من شأنه الحد من عدم تماثل المعلومات، **ويقلل من تكلفة التمويل بالإقتراض**. وقد تؤدي زيادة الوعي بالأمن السيبراني إلى **انخفاض تكلفة الديون** للشركات، وتحسين شروط التعاقد على الديون، وقد **يقيم الدائنين** بشكل إيجابي التدابير والاجراءات الاحترازية للشركات لإدارة المخاطر السيبرانية (Godoy, 2021, p70, 75) .
- **وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المملوك (تكلفة حقوق الملكية)**، حيث أن معامل الارتباط سلبي بقيمة (-0.380)، ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى **انخفاض تكلفة رأس المال المملوك (تكلفة حقوق الملكية)** للشركة، **مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة ارتباط معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المملوك (تكلفة حقوق الملكية) .** **وتتفق هذه النتائج** مع دراسة (Elmawazini et al., 2023)، والتي توصلت إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال المملوك كمقياس لمخاطر المساهمين. حيث أن

الشركات التي تقلل من التعرض للمخاطر السيبرانية تتمتع بانخفاض في تكلفة حقوق الملكية (Ashraf and Sunder , 2023, p14) . **وذلك على عكس** دراسة (Abdollahi et al., 2022)، والتي توصلت إلى أن مخاطر المعلومات لها تأثير إيجابي كبير على تكلفة حقوق الملكية.

- **وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية ومتوسط التكلفة المرجحة لرأس المال (المقترض و المملوك)**، حيث أن معامل الارتباط سلبي بقيمة (-0.487) ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى **انخفاض متوسط التكلفة المرجحة لرأس المال (المقترض و المملوك)، مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة إرتباط معنوية بين الإفصاح عن المخاطر السيبرانية ومتوسط التكلفة المرجحة لرأس المال (المقترض و المملوك)** . حيث أن المعلومات الإضافية تقلل من عدم التأكد لدى المستثمرين، وبالتالي تقلل تكلفة رأس المال، ويؤدي عدم الافصاح عن معلومات موثوقة إلى خلق مشكلة عدم تناسق المعلومات، وهو ما يؤثر على تكلفة رأس المال (Bhatia and Kaur, 2023, p4) . **وبناءً على نظريتي الاشارة والوكالة**، فإن هناك حوافز كبيرة للشركات للافصاح عن المعلومات المتعلقة بالأمن السيبراني لأصحاب المصلحة لتقليل تكلفة رأس المال، ومنع الدعاوى القضائية (Kelton and Pennington, 2020; Firoozi and Mohsni, 2023, p10) . **وتتفق هذه النتائج** مع دراسة (Song et al., 2020)، والتي توصلت إلى أن قيام الشركات بإخطار العملاء بالحوادث السيبرانية، يؤدي إلى زيادة وعي المستثمر للشركة وبالتالي تقليل تكلفة رأس المال، وكذلك توصلت نتائج دراسة (الفقي،2021) إلى وجود علاقة عكسية معنوية بين هيكل رأس المال (LTA) ومستوى إدارة المخاطر الرقمية في البنوك. وتوصلت دراسة (Havakhor et al., 2021)، والتي توصلت إلى أن الإفصاح عن معلومات الأمن السيبراني تقلل من تكلفة رأس المال عن طريق تقليل عدم تناسق المعلومات حول قدرة الشركة على التعامل مع المخاطر السيبرانية. **وهو ما توصلت إليه نتائج** دراسة (Elmawazini et al., 2023)، والتي أكدت على إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال. كما أن الإفصاحات المتعلقة بالأمن السيبراني للشركة ستؤدي أيضاً إلى تقليل عدم تناسق المعلومات بين إدارة الشركة ومستثمريها، وهذا يمكن أن يقلل من تكلفة رأس مال الشركة (Lenka et al., 2023, p176) . **وذلك على عكس** دراسة كل من (الأمير، 2022، ص495؛ McGrath et al., 2022, p9)، والتي توصلت إلى أن الإفصاح عن المخاطر السيبرانية يؤدي إلى زيادة تكلفة رأس المال وكشف المعلومات السرية. وبسبب **الإفصاح المقيد** للشركات التي تم اختراقها، تؤدي إلى زيادة تكلفة رأس المال، من خلال تفاقم عدم تناسق معلومات السوق (Ali et al., 2022, p24-25, 37) .
- **بالنسبة للمتغيرات الرقابية** والتي يتم أخذها في الاعتبار عند الحكم على العلاقة بين الإفصاح عن المخاطر السيبرانية و**التكلفة المرجحة لرأس المال (المقترض و المملوك)**، أكدت النتائج على وجود علاقة موجبة معنوية بين درجة الرفع المالى وبين **التكلفة المرجحة لرأس المال (المقترض و المملوك)**، بينما ارتبطت حجم الشركة بعلاقة سلبية معنوية مع **التكلفة المرجحة لرأس المال (المقترض و المملوك)، وعدم وجود علاقة معنوية بين كل من ربحية الشركة ونسبة اقتناء الأصول غير الملموسة مع التكلفة المرجحة لرأس المال.**
- **وبالنسبة للعلاقة بين المتغيرات الرقابية** وبين مستوى الإفصاح عن المخاطر السيبرانية، أكدت نتائج جدول الارتباط السابق على وجود علاقة موجبة معنوية بين كل من حجم الشركة **ونسبة اقتناء الأصول غير الملموسة** وبين الإفصاح عن المخاطر السيبرانية، وترتبط درجة الرفع المالى سلبياً ومعنوياً مع الإفصاح عن المخاطر السيبرانية، **وعدم معنوية العلاقة بين** ربحية الشركة ومستوى الإفصاح عن المخاطر السيبرانية.

وهذه النتائج **تتفق مع دراسة** (Harris et al., 2023, p198)، والتي توصلت إلى أن **حجم الشركة** يرتبط ايجابياً بحجم الافصاح عن المخاطر السيبرانية، حيث تميل الشركات الكبرى إلى استخدام كلمات أكثر للافصاح عن المخاطر السيبرانية مقارنةً بالشركات الصغيرة. وتوصلت دراسة (Firoozi and Mohsni, 2023, p23) أن الافصاح عن المخاطر السيبرانية يرتبط ايجابياً وجوهرياً بحجم الشركة. وفيما يتعلق **بنسبة الأصول غير الملموسة**، فتتفق النتائج مع دراسة (Harris et al., 2023, p198)، والتي توصلت إلى أن نسبة الأصول غير الملموسة إلى إجمالي الأصول للشركة ترتبط ارتباطاً إيجابياً بكمية الافصاح عن المخاطر السيبرانية. وتوصلت دراسة (Harris et al., 2023, p198) إلى أن **الرافعة المالية** الشركة ترتبط سلبياً بكمية الافصاح عن المعلومات المتعلقة بالمخاطر السيبرانية.

ويعزي الباحث هذا الاختلاف مع بعض الدراسات السابقة، في أن الافصاح عن المخاطر السيبرانية في الشركات محل الدراسة، كانت غالبيته في الجانب الايجابي، بالإضافة إلى تكرار نفس العبارات المتعلقة

بالإفصاح عن المخاطر السيبرانية، واستخدام النغمة الايجابية واللغة المعيارية في الإيضاحات المتممة للقوائم المالية على مدار سنوات الدراسة دون إجراء أى تعديلات عليها.

3/3- تحليل نتائج اختبار الفرض الرئيسى الثالث، حيث ينص الفرض الثالث: يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك، **وينبثق من هذا الفرض عدة فروض فرعية كالتالي:**

1/3/3- يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض.

2/3/3- يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك.

3/3/3- يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على المتوسط المرجح لتكلفة رأس المال.

ولقياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك، 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 :**

1/3/3- تحليل نتائج اختبار الفرض الفرعي الأول، حيث ينص الفرض الفرعي الأول على: يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض.

جدول رقم (14)

نتائج تحليل الانحدار بين متغيرات الفرض الثالث (الفرعي الأول)

المتغيرات المستقلة فى النموذج (مستقلة ورقابية)	نتائج تحليل الإنحدار قبل وبعد إدخال المتغيرات الرقابية (أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض (CD)						
	النموذج	التحليل الأساسى			التحليل الإضافى		
	العلاقة المستهدفة	أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض			أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض في ظل وجود المتغيرات الرقابية		
	الرمز	قيمة B	قيمة T	Sig.	قيمة B	قيمة T	Sig.
المقدار الثابت	B0	0.151	15.466	0.000	0.226	6.064	0.000
الإفصاح عن المخاطر السيبرانية	CRD	0.113-	7.782-	0.000	0.099-	6.489-	0.000
حجم الشركة	SIZE	-	-	-	0.004-	3.153-	0.002
ربحية الشركة	ROA	-	-	-	0.053-	1.763-	0.080
درجة الرفع المالى	LEV	-	-	-	0.014	0.725	0.470
نسبة الأصول غير الملموسة	INTAN	-	-	-	0.005-	0.216-	0.830
القيمة التفسيرية (R^2)		معامل التحديد R^2= 0.318			معامل التحديد R^2 = 0.394		
قيمة F		قيمة F = 60.562			قيمة F = 16.371		
المعنوية الكلية للنموذج		مستوى (SIG.) = 0.000			مستوى (SIG.) = 0.000		

المصدر: نتائج التحليل الاحصائي.

وبالنظر لكل نموذج بشكل مستقل يتضح للباحث ما يلي:

- **بالنسبة للمعنوية الكلية لنماذج الانحدار** التي تمثل الفرض الفرعي الأول (1/3) للدراسة على مستوى التحليل الأساسى والإضافي من خلال تحليل التباين (**ANOVA**) للنموذج ككل، بلغت مستوى المعنوية (0.000)، وهي أقل من (0.05) 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 (0.318)، (0.394) 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 **(تكلفة رأس المال المقترض)** بنسبة 31.8%، بينما تفسر المتغيرات المستقلة (الإفصاح عن المخاطر السيبرانية والمتغيرات الرقابية) التغيرات التى تحدث فى المتغير التابع **(تكلفة رأس المال المقترض)** بنسبة 39.4%.
- **وجود أثر سلبي ذو دلالة إحصائية عند مستوى معنوية (0.01) للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها وهى** (حجم الشركة، ربحية الشركة، درجة الرفع المالى ونسبة الأصول غير الملموسة)، حيث أن معامل الإنحدار سلبي ومستوي المعنوية (sig) أقل من (0.01) .
- **أكدت نتائج الجدول على وجود أثر معنوى سلبي لحجم الشركة علي تكلفة رأس المقترض المملوك، وعدم وجود أثر معنوى للمتغيرات الرقابية الأخرى علي تكلفة رأس المقترض المملوك.**

وفى ضوء نتائج الإنحدار المتعدد لقياس أثر الإفصاح عن لمخاطر السيبرانية علي تكلفة رأس المال المقترض (تكلفة الديون) فى ظل وجود المتغيرات الرقابية، يمكن تكوين معادلة كمية، كما يلي:

$$CD = 0.226 - 0.099\ (CRD) - 0.004\ (SIZE) - 0.053\ (ROA) + 0.14\ (LEV) - 0.005\ (INTAN) + \varepsilon it$$

وبعد تناول الباحث لنتائج الإنحدار يخلص الباحث إلى ثبوت صحة الفرض الفرعي الأول (1/3) للدراسة، والذي ينص على أنه " يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على علي تكلفة رأس المال المقترض (تكلفة الديون) ".

2/3/3- تحليل نتائـــج اختبـــار الفرض الفرعي الثاني، حيث ينص الفرض الفرعي الثاني على: يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك.

جدول رقم (15)

نتائج تحليل الانحدار بين متغيرات الفرض الثالث (الفرعي الثاني 2/3)

المتغيرات المستقلة فى النموذج (مستقلة ورقابية)	نتائج تحليل الإنحدار قبل وبعد إدخال المتغيرات الرقابية (أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك (CE)						
	النموذج	التحليل الأساسى			التحليل الإضافى (وجود المتغيرات الرقابية)		
	العلاقة المستهدفة	أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك			أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك في ظل وجود المتغيرات الرقابية		
	الرمز	قيمة B	قيمة T	Sig.	قيمة B	قيمة T	Sig.
المقدار الثابت	B0	0.436	9.644	0.000	0.206	1.173	0.243
الإفصاح عن المخاطر السيبرانية	CRD	0.317-	4.691-	0.000	0.384-	5.325-	0.000
حجم الشركة	SIZE	-	-	-	0.012	2.189	0.030
ربحية الشركة	ROA	-	-	-	0.086	0.603	0.542
درجة الرفع المالى	LEV	-	-	-	0.066-	0.739	0.461
نسبة الأصول غير الملموسة	INTAN	-	-	-	0.225	1.961	0.047
القيمة التفسيرية (R2)		معامل التحديد R^2 =0.145			معامل التحديد R^2 = 0.213		
قيمة F		قيمةF = 22.005			قيمة F = 6.820		
المعنوية الكلية للنموذج		مستوى (SIG.) = 0.000			مستوى (SIG.) = 0.000		

المصدر: نتائج التحليل الاحصائي.

وبالنظر لكل نموذج بشكل مستقل يتضح للباحث ما يلي:

- **بالنسبة للمعنوية الكلية لنماذج الانحدار** التي تمثل الفرض الفرعي الثاني (2/3) للدراسة على مستوى التحليل الأساسى والإضافي من خلال تحليل التباين (**ANOVA**) للنموذج ككل، بلغت مستوى المعنوية (0.000)، وهي أقل من (0.05) 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 (0.145)، (0.213) على الترتيب، حيث يفسر الإفصاح عن المخاطر السيبرانية بمفرده التغيرات التي تحدث في المتغير التابع **(تكلفة رأس المال المملوك)** بنسبة 14.5%، بينما تفسر المتغيرات المستقلة (الإفصاح عن المخاطر السيبرانية والمتغيرات الرقابية) التغيرات التى تحدث فى **(تكلفة رأس المال المملوك)** بنسبة 21.3% .
- **وجود أثر سلبي ذو دلالة إحصائية عند مستوى معنوية (0.01) للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها وهى** (حجم الشركة، ربحية الشركة، درجة الرفع المالى ونسبة الأصول غير الملموسة)، حيث أن معامل الإنحدار سلبي ومستوي المعنوية (sig) أقل من (0.01)، **ووجود اثر إيجابي لكل من حجم الشركة ونسبة الأصول غير الملموسة على تكلفة رأس المال المملوك (حقوق الملكية)**، حيث أن معامل الانحدار إيجابي ومستوي المعنوية (sig) أقل من (0.05)، **وعدم وجود أثر معنوى لربحية الشركة ودرجة الرفع المالى علي رأس المال المملوك (تكلفة حقوق الملكية)** . وفى ضوء نتائج الإنحدار المتعدد لقياس أثر الإفصاح عن لمخاطر السيبرانية علي رأس المال المملوك (تكلفة حقوق الملكية) فى ظل وجود المتغيرات الرقابية، يمكن تكوين معادلة كمية، كما يلي:

$$CE = 0.206 - 0.384 (CRD) + 0.012 (SIZE) + 0.086 (ROA) - 0.66 (LEV) + 0.225 (INTAN) + \varepsilon it$$

وبعد تناول الباحث لنتائج الإنحدار يخلص الباحث إلى ثبوت صحة الفرض الفرعي الثاني (2/3) للدراسة، والذي ينص على أنه " يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على علي رأس المال المملوك (تكلفة حقوق الملكية) ".

3/3/3- تحليل نتائـــج اختبـــار الفرض الفرعي الثالث، حيث ينص الفرض الفرعي الثالث على: يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على المتوسط المرجح لتكلفة رأس المال.

جدول رقم (16)

نتائج تحليل الانحدار بين متغيرات الفرض الثالث (الفرعي الثالث 3/3)

المتغيرات المستقلة فى النموذج (مستقلة ورقابية)	نتائج تحليل الإنحدار قبل وبعد إدخال المتغيرات الرقابية (أثر الإفصاح عن المخاطر السيبرانية على المتوسط المرجح لتكلفة رأس المال (WACC)						
	النموذج	التحليل الأساسى			التحليل الإضافى (وجود المتغيرات الرقابية)		
	العلاقة المستهدفة	أثر الإفصاح عن المخاطر السيبرانية المتوسط المرجح لتكلفة رأس المال			أثر الإفصاح عن المخاطر السيبرانية على المتوسط المرجح لتكلفة رأس المال في ظل وجود المتغيرات الرقابية		
	الرمز	قيمة B	قيمة T	Sig.	قيمة B	قيمة T	Sig.
المقدار الثابت	B_0	0.241	8.707	0.000	0.199	1.821	0.071
الإفصاح عن المخاطر السيبرانية	CRD	0.223-	5.389-	0.000	0.198-	4.411-	0.000
حجم الشركة	SIZE	-	-	-	0.003-	0.877-	0.382
ربحية الشركة	ROA	-	-	-	0.091	1.029	0.306
درجة الرفع المالى	LEV	-	-	-	0.067	1.217	0.226
نسبة الأصول غير الملموسة	INTAN	-	-	-	0.110	1.539	0.126
القيمة التفسيرية (R^2)	معامل التحديد ^{2} =0.183				معامل التحديد ^{2} = 0.226		
قيمة F	قيمة F = 29.039				قيمة F = 7.353		
المعنوية الكلية للنموذج	مستوى (SIG.) = 0.000				مستوى (SIG.) = 0.000		

المصدر: نتائج التحليل الاحصائي.

وبالنظر لكل نموذج بشكل مستقل يتضح للباحث ما يلي:

- **بالنسبة للمعنوية الكلية لنماذج الانحدار** التي تمثل الفرض الفرعي الثالث (3/3) للدراسة على مستوى التحليل الأساسى والإضافي من خلال تحليل التباين (**ANOVA**) للنموذج ككل، بلغت مستوى المعنوية (0.000)، وهي أقل من (0.05) 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 (0.183)، (0.226) 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 المتوسط المرجح لتكلفة رأس المال بنسبة 18.3%، بينما تفسر المتغيرات المستقلة (الإفصاح عن المخاطر السيبرانية والمتغيرات الرقابية) التغيرات التى تحدث فى المتغير التابع المتوسط المرجح لتكلفة رأس المال بنسبة 22.6% .
- **وجود أثر سلبي ذو دلالة إحصائية عند مستوى معنوية (0.01) للإفصاح عن المخاطر السيبرانية على المتوسط المرجح لتكلفة رأس المال (المقترض والمملوك)، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها وهى** (حجم الشركة، ربحية الشركة، درجة الرفع المالى ونسبة الأصول غير الملموسة)، حيث أن معامل الإنحدار سلبي ومستوي المعنوية (sig) أقل من (0.01) .
- **أكدت نتائج الجدول على عدم وجود أثر معنوى للمتغيرات الرقابية علي المتوسط المرجح لتكلفة رأس المال (WACC) (المقترض والمملوك)**

وفى ضوء نتائج الإنحدار المتعدد لقياس أثر الإفصاح عن لمخاطر السيبرانية علي المتوسط المرجح لتكلفة رأس المال فى ظل وجود المتغيرات الرقابية، يمكن تكوين معادلة كمية، كما يلي:

$$WACC = 0.199 - 0.198 (CRD) - 0.00 (SIZE) + 0.091 (ROA) + 0.067 (LEV) + 0.110 (INTAN) + \varepsilon it$$

وبعد تناول الباحث لنتائج الإنحدار يخلص الباحث إلى ثبوت صحة الفرض الفرعي الثالث (3/3) للدراسة، والذي ينص على أنه " يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على **المتوسط المرجح لتكلفة رأس المال) ". وتتفق** هذه النتائج مع **دراسة كل من (Song et al., 2020; Godoy, 2021)**، والتي أكدت على أن الإفصاح عن الأمن السيبراني يؤدي إلى زيادة وعي المستثمر وبالتالي تخفيض تكلفة رأس المال. **وتتفق** مع دراسة **(Elmawazini et al., 2023)**، والتي توصلت إلى أن متطلبات الإفصاح عن المخاطر السيبرانية تؤدي إلى انخفاض في تكلفة رأس المال كمقياس لمخاطر المساهمين وذو دلالة احصائية عند مستوي معنوية (1%) . **وبناءً** على ما تقدم، **وبعد تناول الباحث لنتائج الانحدار يخلص الباحث إلى ثبوت صحة الفرض الرئيسي الثالث للدراسة، والذي ينص على أنه** " يوجد أثر ذو دلالة إحصائية للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال (المقترض والمملوك) ".

سادساً: 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:

1- اتضح للباحث أهمية دراسة وتحليل أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال 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 مستوي الافصاح عن المخاطر السيبرانية وتكلفة رأس المال، ستختلف بين القطاعات.

2- خلصت نتائج الدراسة التطبيقية، إلى وجود تفاوت في الإفصاح عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات، **حيث بلغت قيمة اختبار (Mann-Whitney Test) (0.009)** وهو أقل من (0.05) 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.

3- **وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض (تكلفة الديون)**، حيث أن معامل الارتباط سلبي بقيمة (-0.564) ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، و**وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المملوك (تكلفة حقوق الملكية)**، حيث أن معامل الارتباط سلبي بقيمة (-0.380)، ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، كما أوضحت مصفوفة الارتباط **وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية ومتوسط التكلفة المرجحة لرأس المال (المقترض و المملوك)**، حيث أن معامل الارتباط سلبي بقيمة (-0.487) ومستوي المعنوية (sig) بلغ (0.000) أقل من (0.01)، حيث كلما توسعت الشركة في الإفصاح عن المخاطر السيبرانية، كلما أدى ذلك إلى **انخفاض متوسط التكلفة المرجحة لرأس المال، مما يدعم صحة الفرض الثاني للدراسة بوجود علاقة إرتباط معنوية بين الإفصاح عن المخاطر السيبرانية ومتوسط التكلفة المرجحة لرأس المال.**

4- أكدت نتائج تحليل الانحدار على **وجود أثر سلبي ذو دلالة إحصائية عند مستوى معنوية (0.01) للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض**، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها، **وأن قيمة معامل التحديد (R^2)** تبلغ (0.318)، (0.394) على الترتيب، **وبالنسبة للإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المملوك**، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها، بلغ معامل التحديد **(R^2)** لنموذج الانحدار، قبل إدخال المتغيرات الرقابية وبعد إدخالها تبلغ (0.145)، (0.213) على الترتيب، **وبالنسبة لقياس أثر الإفصاح عن المخاطر السيبرانية** على **المتوسط المرجح لتكلفة رأس المال "، وجد أن الأثر سلبي وجوهري، وذلك قبل إدخال المتغيرات الرقابية وفى ظل وجودها**، حيث يفسر الإفصاح عن المخاطر السيبرانية بمفرده التغيرات التي تحدث في المتغير التابع المتوسط المرجح لتكلفة رأس المال بنسبة 18.3%، بينما تفسر المتغيرات المستقلة التغيرات التى تحدث فى المتغير التابع المتوسط المرجح لتكلفة رأس المال بنسبة 22.6% .

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

1- ضرورة التحقق من حجم وجودة الإفصاح عن المخاطر السيبرانية، وأن يتضمن الإفصاح 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.
2- ضرورة اهتمام البنوك والشركات المصرية بتعزيز دور أهم العوامل المؤثرة على مستوى الإفصاح عن المخاطر السيبرانية والتي تتمثل في: (حجم البنك/ الشركة، ومؤشرات الربحية وأهمها مؤشر العائد على الأصول، ونسبة الأصول غير الملموسة إلى إجمالي الأصول)، التي قد تؤثر على إدارة وحوكمة هذه المخاطر، مما يساعد ذلك في تخفيض تكلفة رأس المال.
3- ضرورة 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 2030، 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.
4- ضرورة وضع لائحة الضوابط والتعليمات الرقابية المرتبطة بآليات وأُطر تأمين وحماية المنظومات التقنية والتطبيقات الإلكترونية المالية ضد الاختراقات السيبرانية، ومتابعة تعميم ذلك لضمان توفير متطلبات الأمن والجودة عند تطوير أو شراء تلك التطبيقات، وذلك بما يتوافق مع مبادئ وقواعد الحوكمة لهذا الإطار.

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

1- نموذج مقترح لقياس أثر الافصاح عن إدارة المخاطر السيبرانية التشغيلية على التكلفة الضمنية لرأس المال وانعكاس ذلك على الأداء المالي للبنوك التجارية المصرية في ضوء المعايير والاصدارات المهنية الحاكمة.
2- تأثير الافصاح عن برنامج التأكيد المشترك عن المخاطر السيبرانية على جودة تقارير الاستدامة وانعكاس ذلك على تصورات وقرارات المستثمرين.
3- نموذج مقترح للقياس والافصاح عن المخاطر السيبرانية للأصول الرقمية على تكلفة لرأس المال وانعكاس ذلك على مخاطر انهيار أسعار الأسهم.
4- نموذج محاسبي مقترح لقياس تكاليف المخاطر السيبرانية للمنتجات الرقمية في ظل تطبيق عقود الشراكة بين القطاعين العام والخاص (BOT) وانعكاس ذلك على ترشيد القرارات الاستثمارية.

المراجـع

أولاً: المراجع باللغة العربية:

- **المجلات والدوريات العلمية:**

1- أبو الخير, محمد حارس محمد طه. (2023) . 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 15، العدد الأول، مارس، ص1-71.
2- الأمير، شمران عبيد خليف. (2022) . 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، المجلد14، العدد 45، ص486-503.
3- البراشي, أحمد محمود أحمد. (2022) . مدخل مقترح للمحاسبة عن تكلفة الاقتراض وأثره على قرارات المستخدم الخارجي للقوائم المالية: دراسة تطبيقية على الشركات المقيدة في سوق الأوراق المالية المصري .المجلة الدولية للعلوم الإدارية والاقتصادية والمالية، جمعية تكنولوجيا البحث العلميSRTAEG، المجلد الأول، العدد الثالث، ص43-96.
4- الزهيري، احمد خليل، يوسف، ناجي نجيب & الدسوقي, فاطمه محمود. (2022) . العلاقة بين القيود المالية وتكلفة حقوق الملكية في شركات المساهمة المصرية "دراسة إختبارية"."مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق، المجلد44، العدد (1)، ص 178- 206.

5- السواح، نادر شعبان إبراهيم. (2021) . انعكاس جائحة كورونا على نظم الرقابة الداخلية وأثرها على أمن المعلومات بالبنوك التجارية المصرية: دراسة ميدانية .مجلة التجارة والتمويل، كلية التجارة، جامعة طنطا، ع1، ص473-536.
6- السيد، محمد صابر حموده، الجندي، خالد محمد محمد، عيد، السيد عيد محمد. (2023) . أثر جودة حوكمة الشركات والتدفقات النقدية التشغيلية على سرعة تعديل هيكل رأس المال: دراسة تطبيقية. مجلة التجارة والتمويل، كلية التجارة، جامعة طنطا، 43 (1) , 52-104.
7- الشريف، محمود مصطفى منصور. (2023) . قياس مدى تأثير القدرة الإدارية على تكلفة رأس المال المملوك للمنشأة، في بيئة الأعمال المصرية: دراسة عملية. المجلة العلمية للبحوث التجارية، كلية التجارة، جامعة المنوفية، 49 (2) , 543-578.
8- الصاوي, عفت أبو بكر محمد. (2022) . 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، 6 (2) , 35-112.
9- الصيرفي، أسماء أحمد. (2022) . 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، (10-11 مارس2022)، كلية التجارة، جامعة الإسكندرية، ص 1-11.
10- الفقي، رشا علي إبراهيم. (2021) . قياس العلاقة بين هيكل رأس المال ومستوى إدارة المخاطر الرقمية وانعكاسها على الأداء المحاسبي في البنوك – مؤشر مقترح وأدلة تطبيقية من البورصة المصرية، المجلة العلمية للدراسات المحاسبية، كلية التجارة، جامعة قناة السويس،المجلد3، العدد3، ص1-93.
11- النعيمي، فاتن أمين. (2021 (. التحفظ المحاسبي بالقوائم المالية وأثره على تكلفة رأس المال في البنوك التجارية المدرجة في سوق عمان المالي، المجلة العربية للإدارة، مج 41، ع3، ص 195- 204.
12- الوكيل، حسام السعيد. (2022) . أثر تبني المعايير الدولية للتقرير المالي IFRS على العلاقة بين التحفظ المحاسبي وتكلفة رأس المال: دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية .المجلة العلمية للدراسات المحاسبية، مج4, ع2، 651- 724.
13- أميرهم, جيهان عادل ناجى أميرهم. (2022) . 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 23، العدد الثالث، يوليو، ص 325-377.
14- بريك، دعاء أحمد سعيد فارس. (2020) . أثر هيكل الملكية على العلاقة بين مستوى الإفصاح الاختياري وتكلفة رأس المال: دراسة اختبارية على الشركات المساهمة المصرية. مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، المجلد 24، العدد الأول، ص1-57.
15- شحاتة، محمد موسي علي، والبردان، محمد فوزي أمين. (2021) . 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، 2-3 أكتوبر 2021، ص1-25.
16- شرف، إبراهيم أحمد إبراهيم. (2023) . 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، ص211-282.
17- صالح، نرمين محمد شاكر إبراهيم. (2022) . محددات فعالية المراجعة الداخلية للأمن السيبراني". المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة- تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، (10-11 مارس2022)، كلية التجارة، جامعة الإسكندرية، ص 1-24.
18- عازر، رانيا هاني رمزي. (2022) . 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 11، العدد 3، ديسمبر 2022، ص33-71.
19- عثمان، محمد أحمد. (2022) . 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 1-18.

20- عفيفي، هلال عبد الفتاح، فودة، السيد أحمد، عبده، نبيل محمد الشحات. (2021) . 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، ص187-250.
21- عقل، يونس حسن، زهري، علاء فتحي. (2020) . 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 34، العدد الرابع، ص 201-262.
22- على, عايدة محمد مصطفى. (2022) . 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 422-495.
23- علي، محمود أحمد أحمد، علي، صالح علي صالح. (2022) . 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، (10-11 مارس2022)، كلية التجارة، جامعة الإسكندرية، ص 1-64.
24- فرج, هاني خليل. (2022) . 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 11، العدد 2، أغسطس، ص 129- 209.
25- 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.
26- محروس, رمضان عارف رمضان، أبو الحمد، مصطفى صالح. (2022) . استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني. مجلة البحوث المالية والتجارية, كلية التجارة، جامعة بورسعيد، المجلد 23، العدد الثالث، يوليو، ص432-491.
27- مليجى، مجدى مليجى عبدالحكيم. (2017) . "تحليل العلاقة بين الإفصاح المحاسبي عن المعلومات المستقبلية وتكلفة رأس المال وأثرها على كفاءة القرارات الاستثمارية للشركات المصرية"، مجلة المحاسبة والمراجعة، كلية التجارة، جامعة بني سويف، المجلد الخامس، العد الثاني، مايو، ص ص1-55.
28- يعقوب، ابتهاج إسماعيل، وهاب، اسعد محمد علي، و الفرطوسى، علي سموم. (2022) . 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، مج9, ع1، ص 1403- 1430.
29- يوسف, امانى احمد وهبه. (2022) . 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 13، العدد 2، إبريل، ص 28- 109.

- **المواقع الإلكترونية والنشرات:**

1- البنك المركزي المصري (٢٠١٩) . تقرير الاستقرار المالي لعام ٢٠١٨.
2- البنك المركزي المصري. (2021) . التعليمات الرقابية لإدارة مخاطر التشغيل وفقاً لإصلاحات بازل 3 الصادرة في ديسمبر 2017، قطاع الرقابة والإشراف، 4 يناير 2021، ص1-24.
3- البنك المركزي المصري. (2021) . تعليمات خطط التعافي. قطاع الرقابة والإشراف، 2 سبتمبر 2021، ص1-12.
4- البنك المركزي المصري. (2021) . الفصل الثاني القواعد المنظمة لتقديم الخدمات المصرفية عبر الإنترنت. 9 نوفمبر 2019، ص1-36.
5- المركز المصري للدراسات الاقتصادية. (2019) . سلسلة ورش عمل بعنوان " أجندة بحثية تفصيلية لدعم الجهة الحكومي التحول الرقمي للاقتصاد المصري - بحث ودراسة الحالة المصرية: قضايا أفقية"، الورشة الثالثة، فبراير.
6- موقع معلومات مباشر مصر: https://www.mubasher.info/countries/EG
7- موقع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات https://www.egcert.eg/ar/

ثانياً: المراجع باللغة الإنجليزية:

1- Abu-Bader, S. H. (2021) . Using statistical methods in social science research: With a complete SPSS guide. Oxford University Press, USA.
2- Afzal, F., Shehzad, A., Rehman, H. M., Afzal, F., & Mukit, M. M. H. M. H. (2023) . Risk perception and cost of capital in emerging market projects using dynamic conditional correlation model. International Journal of Islamic and Middle Eastern Finance and Management, 16 (2) , 253-273.
3- Alia, M. A., & AbuSarees, A. K. (2023) . Reducing Cost of Capital. Do Voluntary Disclosure and Accounting Conservatism Contribute?. FIIB Business Review, 23197145221145753.
4- Amanullah, A., & Lyu, X. (2022, October) . CORPORATE GOVERNANCE, DISCLOSURE QUALITY, AND COST OF EQUITY: EVIDENCE FROM PAKISTAN. In Proceeding of The International Conference on Economics and Business (Vol. 1, No. 2, pp. 254-268) .
5- Amenya, C. T., & Fon, J. (2022) . ESG and the cost of capital, Does disclosure of ESG performance affect the cost of equity and cost of debt? (Doctoral thesis, OsloMet–Oslo Metropolitan University) .
6- Asauri, Z. A. F. (2022) . Disclosure of Cyber Risk: Its Effect on Banking Profitability in Indonesia (Doctoral dissertation, STIE Indonesia Banking School) .
7- Ashraf, M., & Sunder, J. (2023) . Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws and the cost of equity. The Accounting Review, 98 (4) , 1-32.
8- Ashraf, M., Jiang, J. X., & Wang, I. Y. (2022) . Are There Trade-Offs with Mandating Timely Disclosure of Cybersecurity Incidents? Evidence from State-Level Data Breach Disclosure Laws. Evidence from State-Level Data Breach Disclosure Laws (March 26, 2022) .
9- BCBS. (2018) . Cyber-resilience: Range of practices. Bank For International Settlements. available at: https://www.bis.org/bcbs/publ/d454.htm.
10- Benaroch, M., & Fink, L. (2021) . No Rose without a thorn: Board IT competence and market reactions to operational IT failures. Information & Management, 58 (8) , 103546.
11- Bendriouch, F., Jabbouri, I., Satt, H., Jariri, Z., & M'hamdi, M. (2022) . Tone complexity and the cost of debt retrospective data from the USA. Review of Behavioral Finance, (ahead-of-print) .
12- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018) . Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37 (6) , 508-526.
13- Bhatia, A., & Kaur, A. (2023) . The influence of information asymmetry on the interaction between voluntary corporate disclosure and cost of equity: evidence from publicly traded Indian enterprises. International Journal of Law and Management.
14- 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.
15- CENTRAL BANK OF BAHRAIN. (2021) .Appendix RM-1 Cyber Security Incident Report. Volume 3: Insurance.
16- Chatterjee, C., Agarwal, N., & Agarwal, S. (2024). Data Breach Notification Laws and Cost of Debt. Available at SSRN 4812852.
17- 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.
18- Chong, W. F., Feng, R., Hu, H., & Zhang, L. (2022) . Cyber Risk Assessment for Capital Management. arXiv preprint arXiv:2205.08435.
19- Cortez, E. K., & Dekker, M. (2022) . A Corporate Governance Approach to Cybersecurity Risk Disclosure. European Journal of Risk Regulation, 13 (3) , 443-463.

20- Cram, W. A., Wang, T., & Yuan, J. (2022) . Cybersecurity research in accounting information systems: A review and framework. Journal of Emerging Technologies in Accounting.
21- 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.
22- D'Arcy, J., & Basoglu, A. (2022) . The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. Journal of the Association for Information Systems, 23 (3) , 779-805.
23- Demek, K. C., & Kaplan, S. E. (2023) . Cybersecurity breaches and investors' interest in the firm as an investment. International Journal of Accounting Information Systems, 49, 100616.
24- Dick-Nielsen, J., Gyntelberg, J., & Thimsen, C. (2022) . The cost of capital for banks: Evidence from analyst earnings forecasts. The Journal of Finance, 77 (5) , 2577-2611.
25- Doval, E. (2018) . The cost of capital and financial risk from investors' perspective. Review of General Management, 27 (1) , 90-103.
26- Dow, K. E., Watson, M. W., & Shea, V. J. (2017) . Riding the waves of technology through the decades: The relation between industry-level information technology intensity and the cost of equity capital. International Journal of Accounting Information Systems, 25, 18-28.
27- Duvenhage, F., Smit, A., & Botha, M. (2022) . Cyber Security disclosure in the banking sector: A case of South Africa and China. IBC, 1-21.
28- Eaton, T. V., Grenier, J. H., & Layman, D. (2019) . Accounting and cybersecurity risk management. Current Issues in Auditing, 13 (2) , C1-C9.
29- 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.
30- Eliwa, Y., Aboud, A., & Saleh, A. (2021) . ESG practices and the cost of debt: Evidence from EU countries. Critical Perspectives on Accounting, 79, 102097.
31- Ezat, A. N. (2019) . The impact of earnings quality on the association between readability and cost of capital: Evidence from Egypt. Journal of Accounting in Emerging Economies, , 9 (3) , 366-385.
32- Ferens, A. (2021) . Cybersecurity and cybersecurity in integrated reports and management reports of operators of key services. Accounting Theoretical Journals, (45 (2) , 31-50.
33- Financial Reporting Council. (2022) . FRC Lab Report: Digital Security Risk Disclosure.
34- Firoozi, M., Mohsni, S. (2023) . Cybersecurity Risk Disclosure in the Banking Industry: A Comparative Study. International Journal of Disclosure and Governance. Forthcoming.
35- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023) . Cybersecurity risk. The Review of Financial Studies, 36 (1) , 351-407.
36- Gao, L., Calderon, T. G., & Tang, F. (2020) . Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468.
37- 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.
38- 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.
39- Grüning, M. (2020) . Risk disclosure and the cost of capital: an empirical and comparative analysis between Chinese and German market. (Doctoral dissertation, Department of Accounting and Controlling, Faculty of Economics , TECHNICAL UNIVERSITY ILMENAU
40- Harris, D., Kuzey, C., Naaman, C., & Sahyoun, N. (2023) . Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt?. Journal of Forensic and Investigative Accounting, 15 (2) .

41- 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.
42- Havakhor, T., Rahman, M. S., & Zhang, T. (2021) . Disclosure of Cybersecurity Investments and the Cost of Capital. Available at SSRN 3553470.
43- Héroux, S., & Fortin, A. (2020) . Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. Accounting Perspectives, 19 (2) , 73-100.
44- Huang, X., Janamanchi, B., & Yang, L. (2024). The hidden cost of silence: How delayed cyberattack disclosure erodes firm profitability. Applied Economics Letters, 1-5.
45- Ibrahim, M., Abdulkarim, H., Muktar, J., & Peter, Z. (2021) . The Impact of Cost of Capital on Financial Performance: Evidence from Listed Non-Financial Firms in Nigeria. Global Business Management Review, 13 (2) , 18-34.
46- Ibrahim, S. N. S., Shamsudin, A., Abdullah, S., Ibrahim, M. T., Jaaffar, M. Y., & Bani, H. (2021) . Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia. International Journal of Academic Research in Accounting Finance and Management Sciences, 11 (4) , 10–28.
47- IFRS. (2022, 01 20) . IAS 23 Borrowing Costs. Retrieved from IFRS Foundation.
48- Ismail, T. H., & Obiedallah, Y. R. (2022) . Firm performance and cost of equity capital: the moderating role of narrative risk disclosure quality in Egypt. Future Business Journal, 8 (1) , 1-19.
49- Janvrin, D. J., & Wang, T. (2021) . Linking cybersecurity and accounting: An event, impact, response framework. Accounting Horizons (forthcoming) .
50- Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022) . Firm Use of Cybersecurity Risk Disclosures. Journal of Information Systems, 36 (1) , 151-180.
51- Jiménez, R. G., & Grima, A. Z. (2020) . Corporate social responsibility and cost of equity: literature review and suggestions for future research. Journal of Business, Accounting and Finance Perspectives, 2 (3) , 15.
52- Jin, J., Li, N., Liu, S., & Nainar, S. K. (2023) . Cyber Attacks, Discretionary Loan Loss Provisions, and Banks' Earnings Management. Finance Research Letters, 103705.
53- 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.
54- 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.
55- Kelton, A. S., & Pennington, R. R. (2021) . Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. Journal of Information Systems, 34 (3) , 133-157.
56- Khelil, I. (2023) . Political connections and cost of debt: a meta-analysis. Journal of Financial Reporting and Accounting, (ahead-of-print) .
57- Kovner, A., & Van Tassel, P. (2022) . Evaluating regulatory reform: Banks' cost of capital and lending. Journal of Money, Credit and Banking, 54 (5) , 1313-1367.
58- Krull, J., & Rich, K. (2023) . Revisiting Information Technology Risks. The CPA Journal, 93 (7/8) , 56-59.
59- Kurniasih, A., & Rustam, M. (2022) . Cost of capital and firm value: Evidence from Indonesia. Investment Management & Financial Innovations, 19 (4) , 14-22.
60- Le, H. T. T., Vo, X. V., & Vo, T. T. (2021) . Accruals quality and the cost of debt: Evidence from Vietnam. International Review of Financial Analysis, 76, 101726.
61- 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.
62- Li, H., No, W. G., & Wang, T. (2018) . SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30, 40-

55. Li, T., & Walton, S. (2023) . Business Strategy and Cybersecurity Breaches. Journal of Information Systems, 1-26.
63- Liu, W., & Tian, G. G. (2021) . Controlling shareholder share pledging and the cost of equity capital: Evidence from China. The British Accounting Review, 101057.
64- 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.
65- 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.
66- 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.
67- Mousa, G. A., Elamir, E. A., & Hussainey, K. (2022) . The Effect of Annual Report Narratives on the Cost of Capital in the Middle East and North Africa: A Machine Learning Approach. Research in International Business and Finance, 101675.
68- 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.
69- 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.
70- Napolitano, G. A . (2023) .literature review on the role of cybersecurity in changing management accounting, auditing and governance.
71- Peng, J., & Li, C. W. (2022) . Security breaches and modifications on cybersecurity disclosures. Journal of Accounting and Management Information Systems, 21 (3) , 452.
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- Rasheed, D. M. M. H. (2023) .Direct and Joint Effects of Earnings Quality and Integrated Reporting on the Cost of Capital. Alexandria Journal of Accounting Research, 7 (1) , 1-40.
74- Remeis, K. (2023) . Board Gender Diversity and Cybersecurity Disclosure Characteristics.
75- Rodríguez, L. Z. S. (2023) . Determination of the Weighted Average Cost of Capital (WACC) applied to a COOPAC of Lima Cercado. Journal of business and entrepreneurial studie, 7 (3) ., 14-26.
76- Rosati, P., Gogolin, F., & Lynn, T. (2022) . Cyber-security incidents and audit quality. European Accounting Review, 31 (3) , 701-728.
77- 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.
78- Shad, M. K., Lai, F. W., Shamim, A., McShane, M., & Zahid, S. M. (2022) . The relationship between enterprise risk management and cost of capital. Asian Academy of Management Journal, 27 (1) , 79-103.
79- 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.
80- Shehata, M. A. Z., Moushtaha, M. M., & Ahmed, O. A. (2023). Investigating Risk Disclosure in the Digital Era & its contraction on bank performance.Faculty of Management Sciences.October University for Modern Sciences and Arts, Graduation Project in Accounting II (ACCT461 II).

81- Sharma, K., & Mukhopadhyay, A. (2022) . Cyber-risk assessment and mitigation of DDoS attacks using semi-structured data models.
82- Sheneman , A. G. (2017) . The Effect of Operating Control Failures on the Cost of Capital-Evidence from Data Breaches (Doctoral dissertation, in the Kelley School of Business Indiana University) .
83- 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.
84- Tahat, I. (2022) . Correlation between Cost of Capital, Book Values and Shares Prices: Evidence from Qatar Stock Exchange. Financial Markets, Institutions and Risks, 6 (3) , 40- 48.
85- Tong, S. (2023) .The Effectiveness of Information Disclosure under Cyber Attack. University of Miami Coral Gables, FL 33124
86- Tosun, O. K. (2021) . Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, 1-15.
87- Trautman, L. J., & Newman, N. (2022) . A Proposed SEC Cyber Data Disclosure Advisory Commission.
88- Tsen, E., Ko, R. K., & Slapnicar, S. (2022) . An exploratory study of organizational cyber resilience, its precursors and outcomes. Journal of Organizational Computing and Electronic Commerce, 1-22.
89- Wang, T., Yen, J. C., & Yoon, K. (2022) . Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. International Journal of Accounting Information Systems, 46, 100567.