السنة الرابعة والعشرون/ عدد خاص/ تموز 2026
https://doi.org/10.31272/ijes.v24.1543

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE : 2791-092X Arcif : 0.375

Analysis of the Impact of Cybersecurity Risk Disclosure on Enhancing the Value of Iraqi Banks

تحليل أثر الافصاح عن مخاطر الأمن السيبراني في تعزيز قيمة المصارف العراقية

ايناس عبد الرسول هويدي
Enas Abd Al-Rasool Howaidi
Inas.Abd2206@coadec.uobaghdad.edu.iq

سعاد عدنان نعمان
Suaad Adnan Noaman
suaad.a@coadec.uobaghdad.edu.iq

كلية الادارة والاقتصاد /جامعة بغداد

Abstract

This study aims to highlight the importance of disclosing cybersecurity risks in Iraqi banks by examining the nature of the risks and cyberattacks they face. The research employs a deductive approach for the theoretical framework and an inductive approach—using a checklist as the primary tool—for data collection and analysis through descriptive and inferential statistical methods in the practical component. The findings reveal that bank employees recognize the importance of cybersecurity, while also indicating the presence of substantial challenges that limit the level of risk disclosure. The study focuses on five dimensions of cybersecurity risk disclosure, with the most significant being the dimension of compliance with international regulations and standards, as well as enhancing the dimension of cybersecurity risk response. Other dimensions include governance for the protection of sensitive financial data, in addition to outlining the financial and strategic impact and cybersecurity risk management. In light of the results, the study recommends enhancing the disclosure of cybersecurity risks in financial reports and implementing regular training programs to improve employee preparedness. It also recommends adopting the proposed index for cybersecurity risk disclosure in banks listed on the Iraq Stock Exchange.

Keywords: Disclosure, Cybersecurity Risks, Bank Value.

المستخلص

يهدف البحث إلى إبراز أهمية الافصاح عن مخاطر الأمن السيبراني في المصارف العراقية، من خلال فهم المخاطر والهجمات الالكترونية التي تواجهها بالاعتماد على أسلوب المنهجين الاستنباطي في الجانب النظري والاستقرائي (قائمة الفحص) أداةً رئيسية لجمع البيانات وتحليلها باستخدام الأساليب الإحصائية الوصفية

والاستدلالية في الجانب العملي، إذ أظهرت النتائج إدراك موظفي المصارف لأهمية الأمن السيبراني، إلى جانب وجود تحديات جوهرية تحد من مستوى الإفصاح عن مخاطره. كما ركّز البحث على خمسة أبعاد للإفصاح، كان أبرزها بعد الالتزام والامتثال للتشريعات والمعايير الدولية، وتعزيز بعد الاستجابة للمخاطر السيبرانية. وتطرقت الأبعاد الأخرى منها بعد الحوكمة، لحماية البيانات المالية الحساسة، إلى جانب بيان بعد الأثر المالي والاستراتيجي وإدارة مخاطر الأمن السيبراني. وفي ضوء النتائج، أوصى البحث بضرورة تطوير الإفصاح عن المخاطر السيبرانية في التقارير المالية، وتنفيذ برامج تدريبية منتظمة لرفع جاهزية الموظفين. كما أوصى باعتماد المؤشر المقترح للإفصاح عن مخاطر الأمن السيبراني في المصارف المدرجة في سوق العراق للأوراق المالية.

الكلمات الرئيسية : الافصاح، مخاطر الأمن السيبراني، قيمة المصارف.

المقدمة

تزايدت أهمية الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية للمصارف بشكل لافت في السنوات الأخيرة، مدفوعة بتسارع التقدم التكنولوجي وتطور التهديدات السيبرانية التي تستهدف القطاع المالي أكثر من غيره، فبعد انتقال العمليات البنكية والمالية إلى بيئات رقمية معقدة، أصبحت المصارف عرضةً للهجمات الإلكترونية التي قد تؤدي إلى خسائر مالية مباشرة وتعطل الخدمات الحيوية، وتقويض ثقة الزبائن والمستثمرين بالنظام المالي ككل. تؤكد الدراسات الحديثة أنّ الإفصاح الشفاف والمنظم عن مخاطر الأمن السيبراني وبرامج إدارتها في التقارير المالية يلعب دوراً محورياً في تعزيز موثوقية هذه التقارير، ويساعد في الحد من عدم تماثل المعلومات بين المصارف وأصحاب المصلحة، كما يساهم في بناء ثقة السوق واستقرار أسعار الأسهم وأحجام التداول. وفق أبعاده (حوكمة الأمن السيبراني ، والمخاطر السيبرانية ، والامتثال للمعايير ، والاستجابة للمخاطر ، والأثر المالي والاستراتيجي) في المقابل، فإنّ ضعف الإفصاح أو غيابه قد يؤدي إلى آثار سلبية على قيمة المصارف، ويزيد من حدة التقلبات في السوق المالية، ولاسيما عند وقوع حوادث سيبرانية جسيمة.

1-منهجية البحث ودراسات سابقة

1.1 : منهجية البحث

1.1.1: مشكلة البحث: تتجلى مشكلة الإفصاح عن مخاطر الأمن السيبراني في عدم وضوح كيفية تأثير هذه المخاطر في قيمة المصارف، إذ أنّ ضعف الافصاح عن هذه المخاطر يؤدي إلى فقدان الثقة من قبل المستثمرين والزبائن مما ينعكس سلبا على الأداء المالي ، ويُعتبر الأمن السيبراني عاملاً حيوياً يؤثر بدوره على القيمة السوقية وعلى استقرار الوحدة الاقتصادية وسمعتها، مما يستوجب ضرورة تطوير السياسات لتحسين الشفافية وتعزيز الإفصاح عن مخاطر الأمن السيبراني ومما سبق يمكن صياغة مشكلة البحث الرئيسة من خلال السؤال الاتي:

هل هنالك أثرٌ للإفصاح عن مخاطر الأمن السيبراني في تعزيز قيمة المصارف العراقية

ومن التساؤل الرئيسي لمشكلة البحث يمكن صياغة التساؤلات الفرعية الاتية:

1- هل تدعم المصارف المحلية الإفصاح الشفاف عن مخاطر الأمن السيبراني.

2- هل الافصاح عن مخاطر الأمن السيبراني يؤثر على قيمة المصارف في البيئة المحلية .

1.1.2: أهداف البحث: يعد الإفصاح عن مخاطر الأمن السيبراني ضروريا في ظل تزايد التهديدات السيبرانية التي تواجه الوحدات الاقتصادية . إذ يهدف هذا البحث إلى تحقيق عدة أهداف تؤثر بشكل مباشر على قيمة المصارف المحلية ، ويمكن تلخيصها كما يلي:

1. بيان مفهوم مخاطر الأمن السيبراني من خلال فهم المخاطر والهجمات الالكترونية التي تواجه المصارف وكيفية تأثيرها على الاستقرار المالي وسمعتها.
2. بيان أهمية الافصاح عن مخاطر الأمن السيبراني وتأثيره على قيمة المصارف في البيئة المحلية.

3. تعزيز أهمية الأمن السيبراني ومدى كفاية وإمكانية محتوى الافصاح عن مخاطر الأمن السيبراني على قيمة المصارف مما ينعكس ايجابيا على قيمتها السوقية .
4. الكشف عن واقع مخاطر الأمن السيبراني في المصارف المحلية .
5. بيان تأثير الافصاح عن المخاطر السيبرانية ومدى تأثيرها على قيمة المصارف من الناحية التطبيقية.

1-1-3: فرضية البحث : في ضوء العديد من نتائج الدراسات السابقة التي تدّعي وجود علاقة ايجابية بين الافصاح عن مخاطر الأمن السيبراني وتأثيره على قيمة المصارف ، وفي ضوء تساؤلات البحث وسعيا نحو تحقيق أهدافه يمكن صياغة فرضيات البحث على النحو التالي :
الفرضية الرئيسة: تفصح المصارف عن مخاطر الأمن السيبراني مما يسهم في تعزيز قيمة المصارف المحلية. ومن الفرضية الرئيسة يتم اشتقاق الفرضيات الفرعية الاتية:
1- تدعم المصارف المحلية للإفصاح الشفاف عن مخاطر الأمن السيبراني.
2- يؤثر الافصاح عن مخاطر الأمن السيبراني على قيمة المصارف في البيئة المحلية .

1-1-4: أهمية البحث: يواجه القطاع المصرفي تحدياتٍ جسيمة تتعلق بمخاطر الأمن السيبراني، ولاسيما مع تصاعد الهجمات الإلكترونية، والتي يمكن أن تترتب عليها خسائرٌ مالية كبيرة وفقدان ثقة الزبائن والمستثمرين لذا يصبح فهم تأثير هذه المخاطر على قيمة المصارف أمرًا بالغا الأهمية. ويلعب الإفصاح الشفاف عن إدارة مخاطر الأمن السيبراني دورًا محوريًا في قرارات الاستثمار، اذ يميل المستثمرون إلى تفضيل المصارف التي تُظهر شفافية في التعامل مع هذه المخاطر وتبني استراتيجيات فاعلة للتخفيف منها. ولا يقتصر تأثير هذا الإفصاح على قرارات الاستثمار فحسب، بل يمتد أيضًا إلى أداء المؤسسات المصرفية وسمعتها ، وثقة أصحاب المصلحة. فالمصارف المحلية التي تُفصح عن إجراءاتها الأمنية وتعزز ثقة المستثمرين بقدرتها على حماية بياناتها تكتسب ميزة تنافسية .ومع تزايد انتشار الهجمات الإلكترونية، ينبغي على الوحدات الاقتصادية إعطاء الأولوية للشفافية في الإفصاح عن ممارسات الأمن السيبراني لتعزيز مرونتها وقدرتها على الصمود في مواجهة التهديدات المتزايدة.

1-1-5 : مجتمع وعينة البحث

1. مجتمع البحث: نظرا لمتطلبات البحث تتطلب وجود مجتمع للبحث لاختبار فرضياته فقد تم اختيار مجتمع البحث المتمثل لاحد المصارف العراقية المدرجة في سوق العراق للاوراق المالية .
2. عينة البحث : تمثلت عينة البحث من العاملين في قسم الامن السيبراني و المختصين بنظم المعلومات والمحاسبين الموجودين في المصرف.

1-1-6: منهج البحث: لتحقيق هدف البحث والسعي لاختبار فروضه اعتمدت الباحثتان العديد من المناهج العلمية المختلفة وكالاتي:
1-المنهج الاستنباطي: هو المنهج الذي اعتمدته الباحثتان لدراسة وتأطير الجانب النظري استعانةً بالمراجع العربية والأجنبية ومواقع الانترنت.
2- المنهج الاستقرائي: باستخدام الجانب العملي للبحث من خلال الافصاح عن مخاطر الأمن السيبراني وتأثيره على قيمة المصارف في البيئة المحلية بالاعتماد على استقراء البيانات والمعلومات لعينة البحث

1-1 -7: الأطار الزماني والمكاني:

اولا: الحدود الزمانية : تمت خلال الفترة من 2025 – 2026 .

ثانيا الحدود المكانية : تتمثل الحدود المكانية في أحد مصارف العراق المحلية المدرجة في سوق العراق للأوراق المالية.

2-1 : دراسات سابقة

جدول رقم (1) دراسات سابقة

1-دراسة : عمرو عادل عبد الفتاح موسى / جامعة مدينة السادات – 2024	
عنوان الدراسة	قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك.
نوع الدراسة	بحث منشور - المجلة العلمية للدراسات والبحوث المالية والإدارية - المجلد السادس عشر – العدد الرابع –ديسمبر2024 ، مصر
اهداف الدراسة	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 الالتزام بها والتعرف على الآثار المترتبة عليها، فضلاً عن قياس أثر الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها وكيفية معالجتها على مؤشرات تكلفة راس المال المقترض والمملوك.
اهم استنتاجات الدراسة	اظهرت النتائج: -خلصت نتائج الدراسة التطبيقية، إلى وجود تفاوت في الإفصاح عن المخاطر السيبرانية بين البنوك وشركات الاتصالات وتكنولوجيا المعلومات، من خلال الاختبارات الاحصائية . - وجود علاقة ارتباط سلبية معنوية بين الإفصاح عن المخاطر السيبرانية وتكلفة رأس المال المقترض(تكلفة الديون) - 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.

جدول رقم (2)

2 - دراسة Watkins , 2014	
عنوان الدراسة	The impact of cyber security attacks on the private sector تأثير هجمات الامن السيبراني على القطاع الخاص /2014
نوع الدراسة	بحث منشور _ مجلة جمعية الشؤون الدولية ، بالعدد 3 سنة 2014، جمهورية تيشيك
اهداف الدراسة	معرفة تأثيرات هجمات الامن السيبراني على القطاع المصرفي .
اهم استنتاجات الدراسة	ان اثر هجمات الامن السيبراني على القطاع الخاص يشكل خطرا هائلا على الابتكار والتطور الاقتصادي والامن القومي .
3- دراسة :He Lia, Won Gyun Nob,*, Tawei Wangc (2018)	
عنوان الدراسة	security disclosure guidance and disclosed SEC's cyber security risk factors Cyber ارشادات الإفصاح عن الأمن السيبراني الصادر عن هيئة الأوراق المالية والبورصات و عوامل الخطر المتعلقة بالأمن السيبراني
نوع الدراسة	بحث منشور المجلة الدولية للمعلومات المحاسبية الانظمة -2018
اهداف الدراسة	هدف البحث في مدى فائدة الإفصاح عن مخاطر الأمن السيبراني في قسم عوامل الخطر في ملفات 10 المشار إليها فيما بعد باسم الإفصاح عن مخاطر الأمن السيبراني وتبين فائدة الإفصاح عن مخاطر الأمن السيبراني بأنها "القدرة على مساعدة أصحاب المصلحة في تقييم احتمال وقوع أحداث سلبية مستقبلية أي حوادث خرق الأمن السيبراني. إن فهم المعلومات التي تنقلها الإفصاحات عن المخاطر أمر مهم لأنه يمكن أن يساعد المستثمرين في تقييم مخاطر الأمن السيبراني للشركة وتزويد الجهات التنظيمية بمعلومات حول ما إذا كانت هناك حاجة إلى قواعد تشريعية إضافية لتشجيع الشركات على الكشف عن المزيد من مخاطر الأمن السيبراني لديها.
اهم استنتاجات الدراسة	أوضحت الدراسة أنّ معظم الأبحاث المبكرة في المحاسبة وأنظمة المعلومات ركزت على رد فعل السوق بعد وقوع حوادث الأمن السيبراني، وفحصت عوامل مثل نوع الاختراق والمعلومات التي يتم الإفصاح عنها ، أشارت نتائج جوردون وآخرون (2010) إلى أنّ الإفصاح الطوعي عن تدابير الأمن السيبراني يؤثر إيجابياً على أسعار الأسهم، اذ يكون للإفصاح عن الإجراءات الاستباقية التأثير الأكبر، يليه الإفصاح عن نقاط الضعف التنظيمية .فضلا الى ذلك تركز الدراسة على قدرة الإفصاح المتعلقة بالأمن السيبراني على التنبؤ بوقوع الحوادث مستقبلاً. و تركز على سلوكيات التهديدات وتخصيص الافصاح حسب مستوى المخاطر ،وانعكاسها على السوق والاستثمار. باختصار، توضح الدراسات أن الإفصاح الفعّال عن مخاطر الأمن السيبراني ليس فقط ضرورة تنظيمية بل أداة استراتيجية لتعزيز ثقة السوق، التنبؤ بالحوادث المستقبلية، وتحسين الأداء المالي والاستثماري للشركات.

مصدر الجدول : اعداد الباحثتان

2-1: المحور الاول : الجانب النظري

2-1-1: الافصاح عن مخاطر الأمن السيبراني

1- **الافصاح:** عُرّف الإفصاح على أنّه" :عملية إظهار المعلومات المالية سواء كان كمية أو وصفية، في القوائم المالية أو في الهوامش والملاحظات والجداول المكملة في الوقت المناسب، مما يجعل القوائم المالية غير مضللة وملائمة لمستخدمي القوائم المالية من الاطراف الخارجية، والتي ليس لها سلطة الاطلاع على الدفاتر وسجلات الوحدة الاقتصادية .(القطامية ، 2022: 68) ومن جهة أخرى فقد عرف الافصاح من المفاهيم التي لاقت اهتماماً متزايدا في الفكر المحاسبي للأهمية التي يضطلع فيها، بخاصة مع التطور الذي طرأ على البيئة الخارجية والتي انعكست على الأسواق المالية وحاجة اصحاب المصالح الى معلومات اكثر شفافية لغرض اتخاذ القرارات، الا ان احتياج اصحاب المصالح ومنهم المستثمرون الى معلومات أوسع نتيجة لارتفاع المخاطر والتأكد المرافق لبيئة

الاعمال ولاسيما المعلومات عن المخاطر التي يمكن ان تتعرض لها الوحدات الاقتصادية واثارها الجوهرية الممتدة على الأمد الطويل جعلت الهيئات المحاسبية والمهنية والجهات الأكاديمية في اتجاه واحد لغرض التكيف والتواصل مع هذه المستجدات (اسماعيل،2023: 30). ويتبين مما سبق أنّ الإفصاح المحاسبي، يركز على الطريقة التي يتم بها إظهار وتوصيل المعلومات إلى المستفيدين، بشكل يعكس حقيقة الوضع المالي الصحيح للوحدة الاقتصادية دون تضليل، ويسمح بالاعتماد على تلك المعلومات في اتخاذ قرارات سليمة، ومن هنا يعتبر الإفصاح المحاسبي أحد أدوات الاتصال، اذ بدون الاتصال لن تكون هناك فائدة من مخرجات النظام المحاسبي.

2ـ مفهوم وتعريف الأمن السيبراني: على الرغم من أهمية مفهوم الأمن السيبراني (Cyber Security) وما أثاره من جدل ونقاش عالمي، إلّا أنّه لا يوجد تعريف عام يتفق عليه لهذا الغرض، اذ عرّفته المنظمة الدولية للمعايير (ISO) بأنّه "الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني" (ISO/IEC 270032:2012). وعُرّف أيضا على أنّه "النشاط الذي يؤمّن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن من إمكانية الحد من الخسائر والأضرار الناجمة عن التحقق من المخاطر والتهديدات الإلكترونية، كما يسمح بإعادة الوضع إلى ما كان عليه بأسرع ما يمكن في حالة التحقق والتأكد من هذه المخاطر، ويتيح الى عدم توقف عجلة الإنتاج، وعدم تحول الاضرار الى خسائر دائمة (Alina et al., 2017:510) ويُعرف مفهوم الأمن السيبراني " بأنّه مجموعة من الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به(40: 2018، Li et al) كما عرّفه المعهد القومي للمعايير والتكنولوجيا (National Institute of Standards and Technology بأنّه عملية حماية المعلومات عن طريق منع الهجمات واكتشافها والتصدي لها، وكذلك منع سوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، لضمان توافرها وسلامتها ومصداقيتها وسريتها، وتأمين خصوصية البيانات.(NIST,2018) ومما سبق ترى الباحثتان أنّ الأمن السيبراني يعتبر مفهوم متعدد الأبعاد وله أهمية كبيرة وفوائد في مختلف الوحدات الاقتصادية وليس فقط في القطاع المصرفي، إذ عرفت الباحثتان الامن السيبراني على أنّه عملية مستمرة لحفظ وحماية الأنظمة المتصلة بشبكة الإنترنت متضمنة الأجهزة والبرامج والبيانات من الهجمات الإلكترونية والحفاظ على سرية البيانات وسلامتها وتوافرها ..

2- **أهمية الأمن السيبراني:** في ظل التكنلوجيا المتقدمة، تبرز أهمية الأمن السيبراني في عدة جوانب تتعلق بالحماية الشاملة للأنظمة الالكترونية والبيانات ينبغي ان تستفيد القطاعات المصرفية من برامج الدفاع السيبراني وتتمثل أهمية الأمن السيبراني فيما يلي(السمحان،2020 :12):

1- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.
2- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.
3- حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.
4- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
5- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيقِ مبادئ الأمن السيبراني
6- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

وتؤكد الباحثتان وفقا لما سبق على أنّ الأمن السيبراني يمثل عاملا حيويا في العصر.التقني الحالي، اذ يلعب دورا هاما وحاسمًا في حماية البيانات والأنظمة وضمان دوام الأعمال وبناء الثقة بين المستخدمين عبر الانترنت.

3- **مفهوم مخاطر الامن السيبراني:** يقصد بمفهوم مخاطر السيبرانية بأنّها مخاطر تشغيلية تخص أصول المعلومات والتكنلوجيا والتي لها عواقب تؤثر على سرية او توافر او سلامة المعلومات

او نظم المعلومات مقارنة بفئات المخاطر التي يغطيها التأمين . بالمقابل فإنّ المخاطر السيبرانية تتفق من حيث الخصائص والمسؤولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية(Cebula ، 2010:28).كذلك تعتبر مخاطر الأمن السيبراني (Cybersecurity risk)من أهم المخاطر التي تواجه المصارف، فهي المخاطر التي يمكن أن تواجه المصارف بما فيها رسالة المصرف ورؤيته و شعاره أو سمعته بسبب إمكانية الوصول غير المصرح أو سوء الاستخدام أو تدمير المعلومات (الهيئة المصرية للأمن السيبراني المصري، 2018:116). كذلك تُعرّف مخاطر الأمن السيبراني وفقا للهيئة الوطنية للأمن السيبراني (2018) .بأنّها التهديدات التي تؤثر على عمليات القطاعات المصرفية مما ينعكس سلبا على رؤيتها ،ورسالتها، إدارتها ،صورتها ،سمعتها ،وأصولها وتشمل هذه المخاطر الهجمات الالكترونية التي تهدف إلى إمكانية الوصول غير المصرح به إلى البيانات او تعطيل الأنظمة والذي قد يسبب خسائرا مالية وضررا للسمعة. (الهيئة الوطنية للأمن السيبراني ،2018: 4)كذلك يعكس الأمن السيبراني عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات التقنية ويحتوي على طبقات متعددة من الحماية منتشرة عبر أجهزة الحاسب الآلي أو الشبكات أو البرامج لإنشاء دفاع فعال في مواجهة الهجمات السيبرانية(شحاته والبردان، 9:2021). وفي إطار عمل لجنة بازل الثالثة تعد مخاطر الأمن السيبراني جزءا من المخاطر التشغيلية, وأدخلت اللجنة نظام تصنيف يشتمل علي الحوادث السيبرانية ,وهو ما يؤكّد الترابط المفاهيمي بين المخاطر التشغيلية والسيبرانية(Curti etal.,2021:6)وتعرف مخاطر الأمن السيبراني Cybersecurity risk))بأنّها عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات .(يعقوب واخرون،2022 :5) لذلك يتبين من الصعب تحديد تعريف لمخاطر الأمن السيبراني، إذ إنّ البحث العلمي في هذا الصدد لم يعتمد بعد معياراً، وإنّها في الواقع فئة معقدة من المخاطر ويمكن النظر إلى المخاطر التي تواجهها القطاعات المصرفية في بيئة من الهجمات السيبرانية من ثلاثة جوانب، تتمثل في(:تحديد وتجميع التهديدات السيبرانية، واتخاذ تدابير لتقليلها أو القضاء عليها، وبناء نظام مناسب لحماية المعلومات المحاسبية (Mironchuk and Maletska, 2022:154). وقد تم تحديد الأمن السيبراني في مجال نظم المعلومات المحاسبية AIS لغرض منع الضرر والاستخدام غير المصرح به واستغلال المعلومات والنظم المحاسبية، وكذلك حماية هذه الأنظمة وحوكمتها واستعادتها والحفاظ عليها من أجل تعزيز السرية والنزاهة والتوافر (Cram et al., 2022: 6). ومما سبق ترى الباحثتان في ظل السعي على صياغة مفهوم محدد لمخاطر الأمن السيبراني، اتضح بأنها مخاطر تتعرض لها الوحدات الاقتصادية والمصارف وتسبب خسائرا(مالية وغير مالية)واسعة النطاق وغير متوقعة النتائج وغير مرغوب فيها، نتيجة حدوث تهديدات محتملة غير مؤكدة للإضرار بسرية ونزاهة وتوافر البيانات والمعلومات الخاصة في الفضاء السيبراني، مما يؤثر على قدرتها وعلى تحقيق أهدافها واستمراريتها في حالة وقوع هذه المخاطر.

4- الافصاح عن مخاطر الأمن السيبراني: إنّ الغرض من الإفصاح عن مخاطر الأمن السيبراني هو توفير معلومات دقيقة لأصحاب المصلحة حول مستوى ونطاق مخاطر الأمن السيبراني، في حين أنّ الإفصاح عن المخاطر كان الزاميا، فإنّه قد يكون عاما أيضا تقوم الإدارة بصياغة استراتيجية صياغة الإفصاح، مع مراعاة التكاليف والحوافز المحتملة، تشكل تحدياً كبيراً. في حين فرضت الجهات التنظيمية ضغوطاً متزايدة على الشركات والمصارف التي تفشل في تقديم إفصاح مناسب عن مخاطر الأمن السيبراني، فقد شكك الباحثون والممارسون في مدى إفادة هذا الإفصاح، إذ يعتبر فهم الإفصاح عن مخاطر الأمن السيبراني أمرا بالغا الأهمية، لأنه يمكن أن يساعد المستثمرين في

تقييم مخاطر الأمن السيبراني التي تتعرض لها المصارف وتزويد الجهات التنظيمية بمعلومات حول ما إذا كانت هناك حاجة إلى قواعد تشريعية إضافية .(Li et al., 2018:3)ونتيجة لاختراق الأمن السيبراني، يمكن حدوث الاختراق بأصول المصارف ومعلومات الزبائن، فضلاً عن سمعتها، وهذا يؤدي إلى اضافة تكاليف معالجة كبيرة ومسؤولية قانونية محتملة مما يشعر أصحاب المصلحة بقلق متزايد بشأن الأمن السيبراني، وبالتالي يطالبون بمعلومات إضافية حول حوادث الأمن السيبراني، ولاسيما تلك التي تنطوي على خروقات فعلية (swif et al,2020:197). وعلى الرغم من عدم وجود إلزام صريح بالإفصاح عن مخاطر الأمن السيبراني في الوقت الحالي، إلّا أنّ هناك عدداً من متطلبات الإفصاح قد تفرض التزاماً على المسجلين بالإفصاح لمثل هذه المخاطر، واستنادا للإرشادات يعتمد مستوى ونوع الإفصاح حسب ظروف الوحدة الاقتصادية او المصرف بما في ذلك احتمالية وقوع حوادث إلكترونية وأثر ذلك الاحتمال على المصرف (Barry et al,2022:8)وكذلك تضمن الافصاح عن مخاطر الأمن السيبراني تأثيرا من خلال أتعاب المراجعة إذ أنّ هناك ارتباطا إيجابيا بين الإفصاح عن مخاطر الأمن السيبراني وأتعاب المراجعة الخارجية، بحيث يتطلب وجود مخاطر سيبرانية أعلى أتعابٍ لمراقبة ضمان جودة المراجعة كما أنّ الحماية من العواقب السلبية، يمكن أن يقلل من تأثيرات الهجمات المستقبلية، حيث يوفر معلومات قيمة للمستثمرين والمشرفين حول كيفية التعامل مع هذه المخاطر(متولي ،غريب،2022 :254)يؤثر الإفصاح عن الهجمات والاختراقات السيبرانية على أسعار الأسهم وأحجام التداول اذ تمثل كثير من التغييرات السلبية مؤشرا هاما لرد فعل المستثمرين نتيجة ذلك الإفصاح والذي يؤثر على قيمة المصارف . فعلى الرغم من صعوبة قياس التكلفة الحقيقية للأضرار التي تلحق بالمصارف في كثير من الأحيان إلا أن هذه التغيرات تمثل طريقة فعالة لتقييم الأثر الاقتصادي الفوري للتهديدات والهجمات السيبرانية.(ابو سمك ، 2023 :308)و ترى الباحثتان أنّ الإفصاح عن الأمن السيبراني قد يتمثل في توفير معلومات دقيقة لأصحاب المصلحة حول مستوى ونطاق مخاطر الأمن السيبراني لغرض التحوط من حوادث الأمن السيبراني والحفاظ على أسهم المستثمرين ،فضلا عن الحفاظ على سمعة وقيمة الوحدات الاقتصادية والقطاعات المصرفية كافة.

2-1-2 : أثر الإفصاح عن المخاطر السيبرانية في قيمة المصارف: لقد تناولت عدة دراسات أثر الإفصاح عن إجراءات الأمن السيبراني في الوحدات الاقتصادية ، إذ يمكن للأطراف المعنية من تقييم قدرة الوحدة الاقتصادية على معالجة الهجمات السيبرانية وحماية المعلومات الحساسة، بما يعزز الثقة وبناء السمعة الطيبة، كما يشير إلى جدية الوحدة الاقتصادية في حماية المعلومات الحساسة مثل معلومات الحسابات المصرفية والمعاملات المالية (Fombrun et al., 2015: 3). وتتطلب ممارسات رقابة الوحدات الاقتصادية تحقيق الشفافية في التقارير السنوية والتي تسعى لها الأنظمة المختلفة، اذ أنّ من أهداف المتابعة ترسيخ مبدأ حق المتعاملين مع الوحدات الاقتصادية من مختلف فئات أصحاب المصالح في الوصول إلى معلومات الوحدات الاقتصادية المؤثرة دون الحاجة إلى اتباع اجراءات معقدة .مما يعني أنّ الوحدات الاقتصادية التي تتعرض لهجمات سيبرانية من المفترض عليها إعلام المتعاملين معها بمثل هذا الهجوم كي يتمكنوا من حماية ما يمكن حمايته من معلوماتهم التي قد تكون تسربت، حتى ولو اضطرت إلى إيقاف التعامل مع هذه الوحدات الاقتصادية .ولكن في المقابل، مثل هذا الإفصاح قد يعرض الوحدات الاقتصادية إلى خسائرٍ مادية لا يمكن تعويضها إذا توقف أصحاب المصالح عن التعامل معها .كما أن مثل هذا الافصاح قد يؤدي إلى انخفاض حاد في الأسهم لحظة الكشف عن تفاصيل الهجوم السيبراني مما يعرضها إلى أخطار مالية تؤثر على أدائها المالي .ولذلك ينبغي الافصاح عن مخاطر الأمن السيبراني حمايةً للمتأثرين به . ويعد مجلس الإدارة من أهم الآليات التي تساعد في تطبيق حماية الوحدات الاقتصادية بشكل فعال، إذ يقع على عاتقه وضع السياسات والخطط والإجراءات لتحقيق أهداف الوحدة وإدارة

المخاطر التي تواجهها (Aguilar, 2014:17) ، والتي من شأنها التأثير السلبى على الأداء المالي . كما يقع على عاتقه مسؤولية وضع إستراتيجية لتحديد المخاطر التي تواجه الوحدات الاقتصادية وكيفية إدارتها والحد منها، وكذلك تحديد مستوى المخاطر التي تتعامل معها(دليل حوكمة الشركات المصري،2016: 1-48) وفى كندا أصدر معهد المحاسبين القانونيين الكندي إرشاداتٍ للوحدات الاقتصادية المقيدة بالبورصة بشأن الإفصاح عن مخاطر الأمن السيبراني، والآثار المحتملة للاختراقات والحوادث السيبرانية والتي من المحتمل أن تؤثر على أداء الوحدة الاقتصادية المستقبلي، وإمكانية التخفيف من الحوادث السيبرانية(CPA- Canada, 2017:). 4ويقدّم أثر الافصاح عن المخاطر على قيمة الوحدة الاقتصادية أحداثاً محتملة يمكن أن تزيد أو تقلل من أصول أو قيم الأعمال في الوحدة الاقتصادية لذا ينبغي أن يتضمن الإفصاح عن المخاطر مشاركة المعلومات حول مميزات الوحدات الاقتصادية كافة وعملياتها واستراتيجياتها والمتغيرات الداخلية / الخارجية التي قد تؤثر على النتائج المتوقعة. (Al Smadi,2017:48). كما تعتبر القدرة على مواجهة مخاطر الأمن السيبراني أمرا ضروريا لنجاح الوحدات الاقتصادية ولكي تكون الوحدات الاقتصادية جزءاً فعالاً من حل المخاطر السيبرانية، فمن الضروري أن تجعل تحليل نقاط الضعف أو النعرات الشاملة الرامية وينبغي أن تتناسب تدابير الأمن السيبراني مع مستوى المخاطر التي تم تحديدها وينبغي أن يحدد تقييم المخاطر البيانات والوظائف الأساسية وكذلك أهميتها مع إيلاء اهتمام خاص للأصول ذات القيمة العالية(Savagia & Wang ,2017:2). وتؤدي نتائج اثار حوادث الأمن السيبراني في الخسائر المالية الى تكاليف باهظة. للتعافي أو العلاج، وفي بعض الحالات التقاضي ،ضرر جسيم لخصوصية المستهلكين، مما يؤدي إلى غرامات محتملة، تفرض على أساس اللوائح مثل اللائحة العامة لحماية البيانات التي يمكن أن تصل إلى 20 مليون يورو أو 40%من إجمالي مبيعات المنظمة في جميع أنحاء العالم: ضعف سلامة العمليات التنظيمية، وانتهاك حقوق الملكية الفكرية، وسوء السمعة و يمكن أن تؤثر الحوادث السيبرانية سلبا على الثقة"، وهو مؤشر مهم للغاية لرأس المال الاجتماعي وعامل حاسم للنمو الاقتصادي (Vasiu,2018:176)وانتجت دراسة (الرشيدي،2019) التأثيرات المهمة ، الاول :التأثير على الأسهم، ان انخفاض أسعار الأسهم قد يؤدي الكشف عن الهجمات السيبرانية إلى انخفاض حاد في أسعار الأسهم بسبب القلق المتزايد بين المستثمرين. والثاني: تقلبات التداول، قد لا يؤثر الإفصاح بشكل كبير على أحجام التداول كما هو متوقع، ولكن يمكن أن يزيد من تقلبات السوق قصير الأمد. (الرشيدي،2019: 452). وكذلك تاثير الافصاح وانعكاسه من خلال تحسين الرقابة الداخلية اذ يشجع الإفصاح على تحسين الرقابة الداخلية واعتماد إطارات حديثة مثل (COBIT5) لتلافي اختراقات النظم الالكترونية ومحاولات التلاعب بالمعلومات(منصور،2021 :227). والحماية من العواقب السلبية: يمكن أن يقلل الإفصاح عن مخاطر الأمن السيبراني من تأثيرات الهجمات المستقبلية، اذ يوفر معلومات قيمة للمستثمرين والمشرفين حول كيفية التعامل مع هذه المخاطر، وكذلك تحسين جاذبية الاستثمار اذ يمكن أن يعزز الإفصاح الشافي بتقرير مستقل حول أمان المعلومات وجاذبية الاستثمار للوحدة الاقتصادية من خلال تعزيز موثوقيتها لدى المستثمرين غير المحترفين (متولي،غريب،2022: 255). أثر الإفصاح عن المخاطر السيبرانية على القيمة السوقية للوحدة الاقتصادية بما يخص فحص سلوك سعر السهم أحد العوامل الوكيلة لثقة المستثمرين، لأنه يعكس التكاليف والمخاطر المستقبلية الحالية والمتوقعة المرتبطة بالمخاطر السيبرانية، من منظور المستثمر ولإدارة الوحدة الاقتصادية المتأثرة لأن سعر السهم يعكس قيمة الوحدة الاقتصادية ، وتشير الزيادة الانخفاض في سعر السهم غالباً إلى زيادة انخفاض ثقة المستثمرين في التدفقات النقدية المستقبلية للوحدة الاقتصادية ويمكن أن تؤثر المخاطر السيبرانية على البيانات المالية، نظراً لأن هذه الآثار ينبغي أن تكون جزءاً من القياس الكمي للأثر الاقتصادي لها، وينبغي قياس عوائد الأسهم على مدى جداول زمنية ممتدة تلي لإعلان(Ali and Lai,2022: 26)كما أنّ دراسة التحول الرقمي لتطوير الإفصاح

عن الإجراءات الأمنية السيبراني، يعطي إشارات مفيدة للمستفيدين. اذ يمثل المصارف الرقمية في المصارف تحدياً للمصرف على التكيف مع متطلباته، مثل الحفاظ على سرية السرية والانفتاح على السرية السيبرانية، كما يمثل في نفس الوقت فرصة للتنافس في بيئة رقمية. وقد أوصت الدراسة بأهمية الدراسات الأكاديمية بتأثير الأنشطة التحليلية عن الأمن السيبراني. (الامير، 2022 :488) وتوصلت دراسة (شرف، 2023) والتي ركزت على قياس تأثير الافصاح عن هذه الإجراءات على قرارات المستثمرين المصريين غير المحترفين، اذ خلصت لوجود تأثير معنوي لهذا الإفصاح لتقديمه إشارات قوية تزيد من ثقة المستثمرين تجاه الوحدات الاقتصادية . ويختلف هذا التأثير باختلاف جنس المستثمر وعمره وتأهيله العلمي. وقد أوصت باستمرار وجود إدارة خاصة لمخاطر الأمن السيبراني، مع حث هيئة الرقابة المالية على تعزيز وتطوير الإفصاح عن إجراءات الأمن السيبراني. (شرف، 2023 : 238) وان التغيرات في السوق تؤثر على الإفصاح بالزيادة أو الانخفاض عن المخاطر السيبرانية، و على الرغم من عدم وجود رد فعل كبير في السوق إذا تضمنت التقارير السنوية زيادة في الإفصاح عن المخاطر السيبرانية، بينما إذا تضمن محتوى الإفصاح المتزايد في تقارير الوحدة الاقتصادية تدابير إضافية لإدارة المخاطر ومنع المخاطر، فمن المحتمل أن يكون رد فعل السوق إيجابيا ، ويحدث رد فعل سلبي كبير في السوق إذا قللت الوحدات الاقتصادية المخترقة من الإفصاح عن المخاطر السيبرانية.(Chen et al., 2023: 8-9)كما تستجيب الوحدات الاقتصادية التي تفصح عن المخاطر السيبرانية بشكل أفضل مقارنةً بوحدة اقتصادية اخرى لم تفعل ذلك، ويقدم هذا دليلًا يعكس الضوء الإيجابي على المخاطر النظامية المتعلقة بالأمن السيبراني بقدر ما يتم تحفيز السوق والوحدات الاقتصادية نفسها على دمج هذه التأثيرات في أسعار الأصول، اذ أن تقييم الإدارة للمخاطر السيبرانية، يعزز قدرة الوحدة الاقتصادية على الاستجابة وتقليل عدم تناسق المعلومات، ويجبر الإدارة على أن يكون لديها استراتيجيات طارئة، مما يؤدي إلى التقييم العادل لهذه المخاطر(Alodat, 2024 : 12) وتتأثر الوحدات الاقتصادية بالتأثير السلبي لعدم الإفصاح وهذا عند عدم وجود إرشادات واضحة للإفصاح عن مخاطر الأمن السيبراني يمكن أن يؤدي إلى ضعف الافصاح، مما قد يعكس آثار سلبية على قيمة الوحدة الاقتصادية نتيجة لانخفاض الثقة لدى المستثمرين والزبائن. (يعقوب ،2024: 431).و ترى الباحثتان أنّه لابد من اتخاذ الإجراءات اللازمة للوقاية من الهجمات السيبرانية من خلال إدارة مخاطر الأمن السيبراني والتي تتبع مجلس الإدارة والذى بدوره يقوم بالإفصاح عن تلك المخاطر، اذ يؤدى ذلك إلى تقليل عدم تماثل المعلومات وتحسين الأداء المالي، كما يؤكد على كفاءة وشفافية الإدارة تجاه أصحاب المصالح ، ومن ثم توفير المعلومات اللازمة التي تساعدهم في تقييم الأداء المالي للوحدات الاقتصادية ولاسيما قطاع المصارف و اتخاذ قراراتهم المستقبلية.

2ـ1ـ3: تفعيل الافصاح عن المخاطر الأمن السيبراني في المصارف: أصدرت لجنة تبادل الأوراق المالية الامريكيةSecurities and exchang commission (SEC)دليلا استرشاديا بمتطلبات الإفصاح عن الأمن السيبراني ومخاطره عام 2018 سبقته دليل لعام 2011 (SEC) بعنوان(statement on PROPOSAL mandatory cyber security disclosure)بيان اقتراح الافصاح الالزامي عن الأمن السيبراني وتقترح(SEC)بفرض الإفصاح الالزامي فعلى الوحدات الاقتصادية ان تفصح بتقرير منفصل او مدمج مع تقارير الوحدة وتقترح ان تكون مع تقرير تعليقات الإدارة وترى ان هذا الإفصاح سيعزز في قدرة المستثمرين على تقييم ممارسات الامن السيبراني للوحدات الاقتصادية والابلاغ عن الحوادث السيبرانية والاختراقات، أي أنّها تعتبر فرصة لجعل المستثمرين يقرروا عن أي المخاطر السيبرانية التي يرغبون بتحملهاواعتبرت(SEC) المخاطر السيبرانية من المخاطر الناشئة ولها تأثيرات مالية وتشغيلية وقانونية والحاجة الى تقارير عن الاحداث الجوهرية للمخاطر السيبرانية وقدمت (SEC) النموذج (8K) والذي ينظم من خلال

قسمين يتعلق **الأول:** بالإفصاح بكافة اشكاله عن مخاطر الامن السيبراني (الإبلاغ عن حوادث الامن السيبراني الجوهرية والتقارير الدورية لتقديم تحديثات حول الامن السيبراني وتقارير دورية وتحليلات الإدارة حول هذه المخاطر في تقرير الإدارة . ويتناول القسم الثاني: جودة الاجراءات المتبعة من قبل الإدارة للإفصاح عن مخاطرها وإدارتها للأمن السيبراني واقترح (SEC) في عام2022 بعض التعديلات المقدمة في الإبلاغ المالي عن حوادث الامن السيبراني الجوهرية والتقارير الدورية لتقديم تحديثات حول حوادث الامن السيبراني التي يتم الابلاغ عنها اذ تقترح (SEC) تقارير دورية حول سياسات واجراءات الوحدة الاقتصادية لتحديد مخاطر الامن السيبراني واشراف مجلس الإدارة على مخاطر الامن السيبراني ودور الإدارة في تقييم المخاطر السيبرانية وتحليلها وتنفيذ السياسات واجراءات الامن السيبراني، واقترح تقارير سنوية الزامية فضلا عن تقديم إفصاح الأمن السيبراني في لغة الأعمال (XBRL) وارفقت (SEC) ،هذا الافصاح بقاعدة تشريعية قانونية متمثلة بقانون الاوراق لمخاطر وحوادث الامن السيبراني الامريكي (2011) فضلا عن إرشادات الإفصاح(13 -CF) الأمن السيبراني الصادر 13 ،تشرين الاول ، 2011. متوفر على موقع www.sec.govldivisions/Corpfin/guidance/cfguidance.topic.htm:

1.3: المحور الثاني : الجانب التطبيقي

تطبيق أبعاد الافصاح عن مخاطر الأمن السيبراني

1-1-3 : تحليل استمارة الفحص: لمعرفة اجابات اتجاهات العينة لكل فقرة عن الافصاح عن مخاطر الأمن السيبراني لإحدى المصارف عينة البحث تم اختيار عدد من الموظفين العاملين في قسم إدارة المخاطر المصرفية بشكل عشوائي، وإجراء المقابلات معهم.

2-1-3 : الأدوات الاحصائية المعتمدة في معالجة البيانات: تم استعمال مقياس ليكرت الثلاثي، وكما موضح في الجدول (3)، وقد تم تحديد أوزان نسبية ومن ثم تحليل البيانات على نحو كمي وتفسير النتائج.

الجدول (3) مقياس ليكرت الثلاثي لتحديد مستوى التطبيق

ت	الفقرة	2	1	0
		مطبق	مطبق الى حد ما	غير مطبق

وبعد القيام بتحديد مستوى التطبيق لكل بعد من الابعاد وبالاستناد إلى نتائج قوائم الفحص، يتم استخراج النسبة المئوية لمدى التطبيق وحجم الفجوة من خلال المعادلات الاتية :

1. الوسط الحسابي المرجح = $\frac{\text{مجموع (الوزن} \times \text{التكرار)}}{\text{مجموع التكرارات}}$

2. النسبة المئوية لمدى المطابقة = = $\frac{\text{الوسط الحسابي المرجح}}{\text{(أعلى درجة في المقياس)}}$

3. حجم الفجوة = 1 - النسبة المئوية لمدى المطابقة.

3-1-3: استعراض وتحليل قوائم الفحص Check Lists: تم بناء نموذج مؤشر مقترح يتكون من خمسة أبعاد رئيسة، يندرج تحت كل بعد مجموعة من المؤشرات الفرعية ولأجل قياس الامن السيبراني لأي مصرف او وحدة اقتصادية، إذ لابد من وجود مؤشرٍ لاعتماده في قياس مخاطر الأمن السيبراني وفقا لتلك الأبعاد، ولغرض قياس تلك الأبعاد وجدت الباحثتان أنّ قياسه يكون من خلال قائمة الفحص. وأنّ آلية القياس والترميز باستخدام مقياس ثنائي أو تدريجي، وفق قائمة الفحص على النحو الآتي:

1. حوكمة الأمن السيبراني: تعد حوكمة الأمن السيبراني إطارا تنظيميا يحدّد السياسات والمسؤوليات والضوابط اللازمة لإدارة مخاطر الأمن السيبراني، وضمان حماية المعلومات والأنظمة الرقمية، وتحقيق الامتثال التشريعي، ودعم استمرارية الأعمال واتخاذ القرار الاستراتيجي

داخل المصارف، والجدول(4)يوضح اجابات العينة حول بعد حوكمة الأمن السيبراني، وكما يلي:

الجدول (4) اجابات العينة حول بعد حوكمة الامن السيبراني

ت	الفقرة	مطبق	مطبق الى حد ما	غير مطبق
1	الافصاح عن وجود لجان بالأمن السيبراني ضمن الهيكل التنظيمي.		√	
2	الافصاح عن جود إدارة مختصة بالأمن السيبراني ومسؤوليتها الافصاح في تقاريرها.		√	
3	الافصاح عن وجود تدابير وسياسة أمن سيبراني في المصرف.		√	
4	الافصاح عن دور التدقيق الداخلي في المخاطر السيبرانية.	√		
	الأوزان	2	1	0
	التكرارات	1	3	0
	النتيجة (حاصل ضرب الوزن * التكرار)	2	3	0
	الوسط الحسابي المرجح	1.25		
	النسبة المئوية للمطابقة	%62.5		
	حجم الفجوة	%37.5		

تُشير نتائج جدول حوكمة الأمن السيبراني إلى أنّ مستوى التطبيق جاء متوسطًا، إذ بلغ الوسط الحسابي المرجّح (1.25) وبنسبة مطابقة قدرها (62.5%)، مقابل فجوة تطبيقية نسبتها (37.5%). ويعكس ذلك وجود اهتمام جزئي بمتطلبات الحوكمة السيبرانية داخل المصرف، ولا سيما في ما يتعلق بالإفصاح عن دور التدقيق الداخلي في إدارة المخاطر السيبرانية، الذي عُدّ البند الأكثر تطبيقاً، في المقابل، أظهرت النتائج ضعفاً نسبياً في الإفصاح عن وجود لجان متخصصة وإدارات مستقلة للأمن السيبراني، إضافة إلى محدودية الإفصاح عن السياسات والتدابير المعتمدة، ويُعد هذا المستوى من التطبيق مؤشراً على الحاجة إلى تعزيز البنية التنظيمية للأمن السيبراني، وتطوير آليات الإفصاح والحوكمة، بما يسهم في تقليص الفجوة وتحقيق حماية أفضل للمعلومات والأنظمة الرقمية.

2. مخاطر الأمن السيبراني: تعبّر مخاطر الأمن السيبراني عن التهديدات المحتملة التي تستهدف الأنظمة والشبكات والبيانات الرقمية، وقد تؤدي إلى اختراق المعلومات، وتعطيل العمليات، وخسائر مالية أو تنظيمية للمصارف، الجدول(5)يوضح اجابات العينة حول بعد مخاطر الأمن السيبراني، وكما يأتي :

الجدول (5) اجابات العينة حول بعد مخاطر الامن السيبراني

ت	الفقرة	مطبق	مطبق الى حد ما	غير مطبق
1	الافصاح عن اجراءات الوقاية من الحوادث او الاختراقات والكشف عنها والاستجابة.	√		
2	الافصاح عن انواع التهديدات التي حدثت فعلاً.		√	
3	الافصاح عن منهجية تقييم المخاطر السيبرانية.		√	
4	وجود خطط استمرارية الاعمال والتعافي بشكل دوري.	√		
	الأوزان	2	1	0
	التكرارات	2	2	0
	النتيجة (حاصل ضرب الوزن * التكرار)	4	2	0
	الوسط الحسابي المرجح	1.5		
	النسبة المئوية للمطابقة	%75		
	حجم الفجوة	%25		

تُبيّن نتائج جدول(5)مخاطر الأمن السيبراني أنّ مستوى التطبيق جاء جيدا نسبياً، إذ بلغ الوسط الحسابي المرجّح(1.5)وبنسبة مطابقة قدرها(75%)، مقابل فجوة تطبيقية محدودة نسبياً بلغت (25%). ويعكس ذلك اهتمام المصرف بالإفصاح عن إجراءات الوقاية من الحوادث السيبرانية وآليات الكشف والاستجابة لها، فضلاً عن توافر خطط لاستمرارية الأعمال والتعافي تُعد من المتطلبات الجوهرية لإدارة المخاطر السيبرانية، وفي المقابل، وأظهرت النتائج أنّ الإفصاح عن أنواع التهديدات التي وقعت فعلياً، وكذلك منهجية تقييم المخاطر السيبرانية، ما زال عند مستوى تطبيق جزئي، الأمر الذي يشير إلى حاجة لتعزيز الشفافية في هذا الجانب، وبشكل عام، تُظهر النتائج توجهاً إيجابياً نحو إدارة المخاطر السيبرانية، مع ضرورة تطوير الإفصاح المنهجي لتقليص الفجوة وتحقيق نضج أعلى في إدارة هذه المخاطر.

3. الامتثال والمعايير: يشير الامتثال والمعايير إلى التزام المصرف بتطبيق القوانين والتشريعات

والمعايير الدولية المعتمدة، بما يضمن سلامة الإجراءات، وتوحيد الممارسات، وتقليل المخاطر وتحقيق الشفافية والكفاءة في الأداء المصرفي، الجدول(6)ويوضح اجابات العينة حول بعد الامتثال والمعايير، كما يلي :

الجدول (6) اجابات العينة حول بعد الامتثال والمعايير

ت	الفقرة	مطبق	مطبق الى حد ما	غير مطبق
1	الافصاح عن الالتزام بتعليمات البنك المركزي.	√		
2	وجود نتائج فحص او تقييم المخاطر السيبرانية.	√		
3	وجود الالتزام بالمعايير الدولية (ISO).	√		
4	الافصاح عن برامج التدريب والتوعية.		√	
	الأوزان	2	1	0
	التكرارات	3	1	0
	النتيجة (حاصل ضرب الوزن * التكرار)	6	1	0
	الوسط الحسابي المرجح	1.75		
	النسبة المئوية للمطابقة	%87.5		
	حجم الفجوة	%12.5		

تُظهر نتائج جدول(6)أنّ مستوى التطبيق جاء مرتفعاً، إذ بلغ الوسط الحسابي المرجّح(1.75) وبنسبة مطابقة بلغت(87.5%)مقابل فجوة محدودة قدرها(12.5%)ويعكس ذلك التزام المصرف الواضح بتعليمات البنك المركزي، وحرصه على إجراء فحوصات وتقييمات للمخاطر السيبرانية، فضلاً عن الالتزام بالمعايير الدولية ذات الصلة، ولا سيما معايير ISO. ويُعد هذا المستوى مؤشراً إيجابياً على قوة الإطار الرقابي والتنظيمي المعتمد في إدارة المخاطر السيبرانية. في المقابل، أظهرت النتائج أن الإفصاح عن برامج التدريب والتوعية ما زال عند مستوى تطبيق جزئي، الأمر الذي يشير إلى ضرورة تعزيز بناء القدرات البشرية ونشر الوعي الأمني بين العاملين. وبشكل عام، تؤكد النتائج وجود بيئة امتثال قوية، مع الحاجة إلى استكمال متطلبات التوعية لضمان استدامة الامتثال وفعاليته. وهذا ما يؤيد إثبات فرضية البحث الأولى التي نصت (تدعم المصارف المحلية للإفصاح الشفاف عن مخاطر الأمن السيبراني) من خلال تحليل الأبعاد (الحوكمة ، ومخاطر الأمن السيبراني والامتثال للمعايير) التي جاءت بشكل متوسط نسبيا في الافصاح عن المخاطر .

4. الافصاح عن الاستجابة للحوادث السيبرانية: هو قيام المصرف بالإفصاح المنهجي عن الإجراءات المتخذة لرصد الحوادث السيبرانية واحتوائها ومعالجتها والتعافي منها، بما يعزز الشفافية، ويدعم الامتثال، ويحد من الآثار التشغيلية والمخاطر المستقبلية. الجدول(5) يوضح اجابات العينة حول بعد الافصاح عن الاستجابة للحوادث السيبرانية، وكما يأتي :

الجدول (7) اجابات العينة حول بعد الافصاح عن الاستجابة للحوادث السيبرانية

ت	الفقرة	مطبق	مطبق الى حد ما	غير مطبق
1	الافصاح عن حوادث سيبرانية سابقة.		√	
2	خطط استجابة من قبل الادارة المختصة للامن السيبراني واجراءات المعالجة المتخذة.	√		
3	الافصاح عن اثر الحوادث على قيمة وسمعة المصرف.		√	
4	الافصاح عن الخسائر المترتبة.			√
	الأوزان	2	1	0
	التكرارات	1	2	1
	النتيجة (حاصل ضرب الوزن * التكرار)	2	2	0
	الوسط الحسابي المرجح	1.33		
	النسبة المئوية للمطابقة	%66.67		
	حجم الفجوة	%33.33		

تشير النتائج في جدول(7)أنّ مستوى التطبيق جاء متوسطاً، إذ بلغ الوسط الحسابي المرجّح (1.33) وبنسبة مطابقة قدرها(66.67%)مقابل فجوة تطبيقية بلغت(33.33%). ويعكس ذلك وجود اهتمام نسبي بالإفصاح عن خطط الاستجابة للحوادث من قبل الإدارة المختصة في المصرف بالأمن السيبراني والإجراءات المتخذة لمعالجتها، وهو ما يُعد جانباً إيجابياً في إدارة الحوادث السيبرانية. وفي المقابل، أظهرت النتائج ضعفاً واضحاً في الإفصاح عن الخسائر المترتبة على الحوادث، فضلاً عن محدودية الإفصاح عن الآثار التي تمس قيمة المصرف

وسمعته، اضافة إلى الإفصاح الجزئي عن الحوادث السابقة. ويشير هذا المستوى من التطبيق إلى حاجة المصرف لتعزيز الشفافية في الإفصاح عن آثار الحوادث السيبرانية ونتائجها المالية والتنظيمية، بما يسهم في تقليص الفجوة، وتعزيز الثقة، وتحسين نضج إدارة الاستجابة للحوادث السيبرانية.

5. الأثر المالي والاستراتيجي: يشير بعد الأثر المالي والاستراتيجي إلى الإفصاح عن ارتباط الأمن السيبراني بالاستراتيجية العامة، وتكاليفه، والاحتياطات والمخصصات المرتبطة به، إضافة إلى بيان الأثر المتوقع للحوادث السيبرانية في القيمة السوقية للمصرف مستقبلاً. الجدول(8) يوضح اجابات العينة حول بعد الاثر المالي والاستراتيجي، وكما يأتي :

الجدول (8)اجابات العينة حول بعد الاثر المالي والاستراتيجي

ت	الفقرة	مطبق	مطبق الى حد ما	غير مطبق
1	ربط الامن السيبراني بالاستراتيجية.	√		
2	الافصاح عن تكاليف الامن السيبراني.		√	
3	الافصاح عن الاحتياطات والمخصصات المرتبطة.	√		
4	الافصاح عن الاثر المتوقع في القيمة السوقية مستقبلاً.		√	
	الأوزان	2	1	0
	التكرارات	2	2	0
	النتيجة (حاصل ضرب الوزن * التكرار)	4	2	0
	الوسط الحسابي المرجح	1.5		
	النسبة المئوية للمطابقة	%75		
	حجم الفجوة	%25		

تشير نتائج جدول(8)أنّ مستوى التطبيق جاء جيداً نسبياً، إذ بلغ الوسط الحسابي المرجّح (1.5) وبنسبة مطابقة بلغت(75%)، مقابل فجوة تطبيقية مقدارها(25%)ويعكس ذلك وجود توجه واضح لدى المصرف لربط الأمن السيبراني بالاستراتيجية العامة، إضافة إلى الإفصاح عن الاحتياطات والمخصصات المرتبطة به، وهو ما يدل على إدراك نسبي للأبعاد الاستراتيجية والمالية للمخاطر السيبرانية. وفي المقابل، أظهرت النتائج أن الإفصاح عن تكاليف الأمن السيبراني، وكذلك الإفصاح عن الأثر المتوقع للحوادث السيبرانية في القيمة السوقية مستقبلاً، ما زال عند مستوى تطبيق جزئي، الأمر الذي يشير إلى حاجة لتعزيز الشفافية المالية والاستشرافية في هذا الجانب. بشكل عام، تعكس النتائج أهمية تطوير الإفصاح الاستراتيجي والمالي للأمن السيبراني بما يسهم في دعم اتخاذ القرار وتحقيق الاستدامة المصرفية. وهذا ما يؤيد اثبات فرضية البحث الثانية التي تنص (يؤثر الافصاح عن مخاطر الامن السيبراني على قيمة المصارف في البيئة المحلية)من خلال تحليل الابعاد الاخرى(الاستجابة للحوادث السيبرانية، والاثر المالي والاستراتيجي)التي جاءت عند مستوى تطبيق جزئي ، فضلا عن الافصاح الجزئي عن الحوادث السابقة التي تؤثر على قيمة المصرف.

4-1-3: التمثيل البياني لنسب المطابقة: استناداً إلى نتائج قوائم الفحص اعلاه، والتي قامت بتقييم مستوى التطبيق لمحاور قائمة الفحص، سيتم عرض النتائج المجمعة من خلال حساب المتوسط الحسابي المرجح لكل محور من المحاور الخمسة، كما هو موضح في الجدول(7):

الجدول (9) ملخص نتائج مستوى التطبيق في المصرف

ت	اسم المحور	الوسط الحسابي المرجح	نسبة المطابقة	حجم الفجوة
1	حوكمة الامن السيبراني	1.25	62.5%	37.5%
2	مخاطر الامن السيبراني	1.5	75%	25%
3	الامتثال والمعايير	1.75	87.5%	12.5%
4	الافصاح عن الاستجابة للحوادث السيبرانية	1.33	66.67%	33.33%
5	الاثر المالي والاستراتيجي	1.5	75%	25%
	نسبة النتائج الاجمالية		73.33%	%26.66

المصدر: من اعداد الباحثتان.

يُظهر جدول(9)أن مستوى تطبيق متطلبات الأمن السيبراني في المصرف جاء جيداً بشكل عام بنسبة مطابقة إجمالية بلغت(73.33%)مع تميز محور الامتثال والمعايير بأعلى مستوى تطبيق

في حين برزت فجوات نسبية في حوكمة الأمن السيبراني والإفصاح عن الاستجابة للحوادث، مما يستدعي تعزيز الأطر التنظيمية للإفصاح لتقليص الفجوة وتحسين الجاهزية السيبرانية.

5-1-3: مخطـط بـاريتو: تعتمد عملية التحليل الفعال على نماذج ومخططات تساعد في تشخيص المحاور المؤثرة على مختلف الظواهر بدقة ووضوح. ومن بين هذه الأدوات، يعد مخطط باريتو تقنية شائعة الاستخدام لتصنيف المعلومات بيانياً من الأكثر إلى الأقل صلة تهدف هذه الطريقة إلى تحديد أهم المشكلات التي تستحق التركيز وحلها بشكل ملح. يعتمد مخطط باريتو على مبدأ باريتو المعروف أيضاً باسم قاعدة (80/20)، والذي ينص على أن 80% من النتائج تأتي من 20% من الأسباب. وبالتالي، يساعد هذا المخطط في تحديد المحاور القليلة التي تساهم بشكل كبير في إحداث المشكلات، مما يتيح اتخاذ قرارات فعالة لحلها. يساعد في تحديد أهم الأسباب أو المشكلات التي تمثل معظم المشكلات، لإنشاء مخطط باريتو، هناك عدد من الإجراءات أهمها :

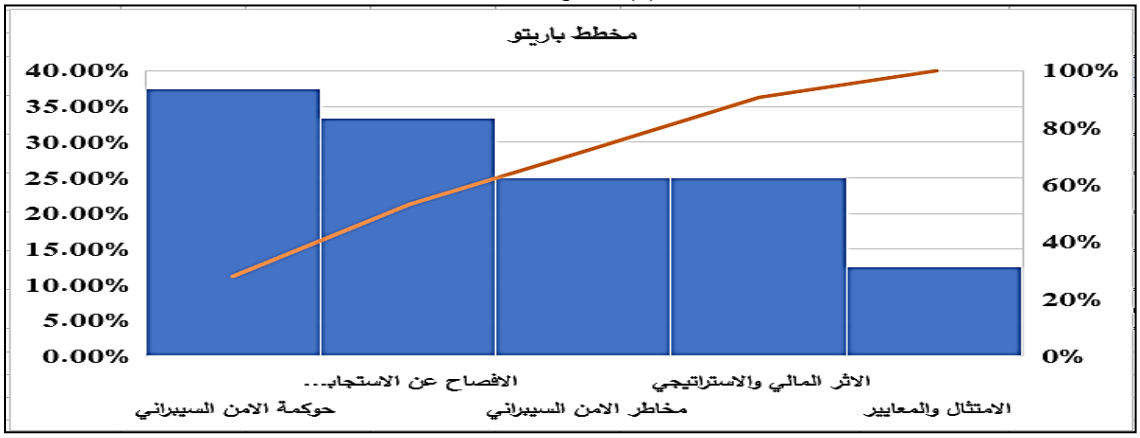
- تحديد المشكلة بوضوح أو القضية التي تريد البحث عنها.
- ثم نقوم بجمع البيانات ذات الصلة لكل فئة أو عنصر.
- يتم ترتيب البيانات أو العناصر بترتيب تنازلي بناء على مساهمتها في المشكلة.
- استخراج النسبة المئوية المعدلة باستعمال القانون (الجزء / الكل × 100).
- القيام بإجراء حساب النسب التراكمية يعكس مدى مساهمة كل مجال في المشكلة الشاملة.
- رسم المخطط البياني إنشاء مخطط عمودي مع الفئات الموجودة على المحور الأفقي والترددات أو المقادير على المحور الرأسي.
- القيام بتحليل مخطط باريتو لتحديد المحاور القليلة الحيوية التي تساهم أكثر في المشكلة التركيز على معالجة هذه المتغيرات ليكون لها التأثير الأكثر أهمية على تغيير الوضع. ومن خلال تلك الإجراءات تكون النتائج كما هي مبينة في الجدول(10):

الجدول (10) حجم الفجوات والنسبة المئوية التراكمية

ت	اسم المحور	حجم الفجوة	النسبة المئوية	النسبة المئوية التراكمية
1	حوكمة الامن السيبراني	37.5%	28.13%	28.13%
2	مخاطر الامن السيبراني	25%	18.75%	46.88%
3	الامتثال والمعايير	12.5%	9.38%	56.25%
4	الافصاح عن الاستجابة للحوادث السيبرانية	33.33%	%25	81.25%
5	الاثر المالي والاستراتيجي	25%	18.75%	100%
	المجموع	133.33%	%100	

المصدر : اعداد الباحثتان

الشكل (1) يوضح مخطط باريتو



المصدر : اعداد الباحثتان

استناداً إلى الجدول(10)ومخطط باريتو في الشكل(1)، يتضح أنّ محوري حوكمة الأمن السيبراني

والإفصاح عن الاستجابة للحوادث السيبرانية يشكلان معاً النسبة الأكبر من حجم الفجوة، إذ يساهمان بما يقارب 53% من إجمالي الفجوة التراكمية، ويشير ذلك إلى أن التركيز على تحسين هذين المحورين سيحقق الأثر الأكبر في تقليص الفجوة الكلية وتعزيز مستوى الجاهزية السيبرانية، كما تظهر بقية المحاور فجوات أقل نسبياً، ما يعكس تقدماً مقبولاً فيها، مع استمرار الحاجة إلى تحسين تدريجي لتحقيق تكامل شامل في تطبيق متطلبات الأمن السيبراني في المصرف المبحوث.

6.1.3: الاستنتاجات والتوصيات

1 : الاستنتاجات

- تظهر أهمية الأمن السيبراني للوحدات الاقتصادية ولاسيما المصارف في البيئة المحلية يسهم في تأمين المعلومات المالية وضمان حمايتها وسلامتها الالكترونية .
- عدم الإفصاح عن المخاطر السيبرانية في البيئة المحلية ولاسيما في التقارير المالية قد يشير إلى تقييم غير دقيق لتلك المخاطر التي قد تواجه المصارف المحلية، مما ينعكس سلبا على الاستعداد لمواجهتها وبالتالي فقدان ثقة المستثمرين .
- تشير النتائج بالنسبة لبعدي الحوكمة و الإفصاح عن الاستجابة لمخاطر الأمن السيبراني اذ جاءت بمستوى تطبيق متوسطا اي اهتمام جزئي بمتطلبات الحوكمة واستجابة للمخاطر ، مما يستدعي الحاجة الى تعزيز الأطر التنظيمية وتطوير آليات الإفصاح والحوكمة، والاستجابة لتقليص الفجوة وتحسين الجاهزية السيبرانية ، اما نتائج الابعاد الاخرى (مخاطر الامن ،والاثر المالي) تشير بمستوى تطبيق جيد بشكل عام نسبيا ، و اخيرا نتائج بعد الامتثال للمعايير جاءت بأعلى مستوى للتطبيق تؤكد النتائج وجود بيئة امتثال قوية لتعليمات البنك المركزي، وحرصه على إجراء فحوصات وتقييمات للمخاطر السيبرانية.

2: التوصيات

- اعتماد وتضمين التقرير السنوي لمخاطر الأمن السيبراني لعرض البيانات والمعلومات بكل شفافية وموثوقية من قبل القطاع المصرفي من شأنه أن يزيد ثقة المستخدمين بمعلوماتهم المالية وتحسين الاداء.
- حث العاملين في القطاع المصرفي على مشاركة دورات توعية وتدريب دوري لجميع الموظفين حول ممارسات الامن السيبراني بما في ذلك كيفية التعامل مع البيانات الحساسة وتجنب الهجمات الاحتيالية اذ يساهم ذلك في تقليل مخاطر الاختراقات والتسريبات مما يعزز الثقة بين المصرف وزبائنه ويحافظ على سمعتها.
- تبني المؤشر المقترح للإفصاح عن مخاطر الأمن السيبراني في تقارير المصارف المدرجة في سوق

العراق للأوراق المالية وفق التعليمات والمعايير المنظمة للإفصاح عن المخاطر السيبرانية.

المصادر REFERENCES

1. أبو سمك، أحمد محمد على ،(قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة تطبيقية من البنوك المصرية المدرجة) كلية التجارة ،جامعة قناة السويس، مصر(2023)ص11.
2. اسماعيل ،رواء، عبد الامير ، (قياس مستوى الافصاح عن المخاطر غير المالية السيبرانية والبيئية على وفق مؤشر مقترح في سوق العراق للاوراق المالية)جامعة المستنصرية ،(2023)ص:30.
3. الامير . م.م شمران عبيد خليف ، (اثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني) مديرية تربية واسط (2022).

4. الامير . م.م شمران عبيد خليف ، (اثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني) ،(2022) مديرية تربية واسط .
5. الرشيدي، طارق عبد العزيز، عباس، داليا عادل ،أثر الإفصاح عن مخاطر الأمن السيبرانى في التقارير المالية على أسعار الأسهم وأحجام التداول : دراسة مقارنة في قطاع تكنولوجيا المعلومات.(2019) .مجلة المحاسبة والمراجعة، كلية التجارة، جامعة بني سويف، المجلد 8 ، العدد الثاني، ص487 – 439
6. السمحان ، منى عبدالله ، (متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود) ،(2020) مجلة كلية التربية، جامعة المنصورة ،العدد111 ، .
7. شحاتة والبردان ، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل إستراتيجيا الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، 2021، جامعة مدينة السادات.
8. شرف إبراهيم أحمد إبراهيم ، أثر افصاح عن إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين (2023)- دراسة تجريبية ، مجلة الإسكندرية للبحوث المحاسبية ، قسم المحاسبة والمراجعة، كلية التجارة، جامعة الاسكندرية، العدد الأول، المجلد السابع ص ٢١١ – ٢٨٢.
9. القطامية ، انصاف جمعة بركات ("أثر الافصاح المحاسبي في القوائم المالية للمؤسسات الحكومية" الاصدار الخامس - العدد تسعة وأربعون تاريخ الاصدار: 2 – تشرين الثاني – 2022م .
10. متولي وغريب ،مصطفي زكي حسين &د/ حسين عبد العال سالم (قياس تأثير الافصاح عن مخاطر الامن السيبراني على أتعاب المراجعة الخارجية :دراسة تطبيقية ،كلية التجارة – جامعة قناة السويس (2022).
11. موسى، عمرو عادل عبد الفتاح / جامعة مدينة السادات (قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال المقترض والمملوك. - المجلة العلمية للدراسات والبحوث المالية والإدارية - المجلد السادس عشر – العدد الرابع –ديسمبر2024 .
12. الهيئة العامة للرقابة المالية، الدليل المصري لحوكمة الشركات(الإصدار الثالث أغسطس) 2016 ، مركز المديرين المصري، 48 - 1 .
13. الهيئة الوطنية للامن السيبراني (الضوابط الاساسية للامن السيبراني.(ECC-1:2018) .
14. الهيئة الوطنية للأمن السيبراني المصري،(116،2018) .
15. يعقوب ، ابتهاج اسماعيل ،واخرون (مؤشر مقترح للافصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للاوراق المالية وفق المتطلبات الدولية)جامعة المستنصرية /كلية الادارة والاقتصاد مجلة الدراسات المالية والمحاسبية والادارية ،المجلد 9 ،العدد1 ،جوان ، 2022 ص5.
16. Al Smadi, Safaa Adnan. "Corporate governance and Risk disclosures practices in the annual reports of Jordanian banks." . 2017, University of Southampton.
17. Aguilar, L. A.." Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus", Cyber Risks and the Boardroom Conference, New York Stock Exchange, (June 10) (2014),. New York, NY: SEC. 1-17
18. Ali, S. E. A., Lai, F. W., Aman, A., Saleem, M. F., & Hamad, S. Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk?.. JOURNAL OF COMPETITIVENESS, (2022) 14(1), 23-42.
19. Alina, C. M. Internal audit role in cybersecurity. Economic Sciences Series. (2017). (XVII) 2: 510 -513.
20. Alodat ,Ahmad Yuosef Alodat1 , Yunhong Hao1, Board characteristics and cybersecurity disclosure: evidence from the UK ,2024, 13 May
21. Barry, T., Jona, J., & Soderstrom, N. The impact of country institutional factors on firm disclosure: Cyber security disclosures in Chinese cross-listed firms. Journal of Accounting and Public Policy(2022). ,41, 1-15.
22. Cebula , J.J. and L.R. Young: "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University,
23. Chen, J., Henry, E., & Jiang, X. Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. Journal of Business Ethics, 1-26. (2023).

24. CPA Canada, Cyber security risks and incidents: Reassessing your disclosure practices,(2017).
25. Curtis, F., Garlic, J., Kazinnik, S., Lee, M. J., & Mihov, A. "Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis", August, mimeo. (2022).
26. cybersecurity risk factors, He Lia, Won Gyun Nob, Tawei Wangc,(2018).
27. Fombrun, C. J., Ponzi, L. J., & Newburry, W.. Stakeholder Tracking & Analysis: The RepTrakR System for Measuring Corporate Reputation. Corporate Reputation Review, 18, 3-24. (2015) https://doi.org/10.1057/crr.2014.21.
28. He Li a ,Won Gyun No b , Tawei Wang .SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. .(2018).
29. ISO/IEC 27032. Information technology – Security techniques – Guidelines for cybersecurity. (2012).
30. Mironchuk, Z. P., & Maletska, O. IORGANIZATION OF ACCOUNTING PROTECTION IN CYBER SECURITY INFORMATION. Actual problems of modern business: accounting, financial and management aspects, . (2022). 152-155.
31. National institute of standards and technology (NIST). a lossary of key information security terms National institute of standards and technology interagency or internal report, .(2018) Available athttp://csrc.nist.gov /publications.
32. Ramírez, M., Rodríguez Ariza, L., & Gómez Miranda, M. E. The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability ,(2022), 14(3), 1390.
33. Savaglia, J. & Wang, P. Cybersecurity vulnerability analysis via virtualization. Issues in Information Systems, (2017). 18(4), 91-98.
34. SEC's cybersecurity disclosure guidance and disclosed
35. Swift, O., Colon, R., and Davis, K.. The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures. Journal of Forensic and Investigative Accounting(2020), 12(2), 197–212
36. Vasiu ,Ioana Vasiu1, Lucian Vasiu2, Cybersecurity as an Essential ustainable Economic Development Factor, European Journal of Sustainable Development (2018), 7, 4, 171-178.
37. Watkins , The impact of cybersecurity attacks on the private sector, Briefing Paper 3/2014, Association for International Affairs,
38. www.sec.govldivisions /Corpfin/guidance/cfguidance.topic.htm.