مجلة الدراسات المالية والمحاسبية والإدارية
ISSN 2352-9962/E-ISSN 2572-0147
المجلد09 العدد 01– جوان 2022

OEB Univ. Publish.

مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية

A Proposed Indicator for Accounting Disclosure of Cyber Risks in the Iraqi Stock Market According to International Requirements: Test Study

ا.د. ابتهاج اسماعيل يعقوب[1]*، ا.د. اسعد محمد علي وهاب[2]، د. علي الفرطوسي[3]

[1] الجامعة المستنصرية - hussainalaa10000@uomustansiriyah.edu.iq

[2] جامعة كربلاء-كلية الإدارة والاقتصاد، asaad.m@uokerbala.edu.iq

[3] الجامعة المستنصرية-كلية الإدارة والاقتصاد، Ali004387@gmail.com

تاريخ التسليم: 11-04-2022 تاريخ المراجعة: 22-05-2022 تاريخ القبول:08-06-2022

الملخص

يهدف البحث الى اقتراح مؤشر للإفصاح عن المخاطر السيبرانية ضمن المعلومات المفصح عنها في التقارير السنوية التي تصدرها الوحدات الاقتصادية وبحكم غياب التعليمات المنظمة لهكذا نوع من الافصاحات في العراق وتراجع مركز العراق في المؤشر العالمي للأمن السيبراني الى المركز (١٢٩)عالميا من اصل (١٨٤) على الرغم من الاهتمام المتزايد من قبل الدولة العراقية بوضع استراتيجية للأمن السيبراني (2018) وعلى وفق ذلك تم بناء مؤشر للإفصاح المحاسبي عن مخاطر الامن السيبراني على وفق المتطلبات الدولية الصادرة عن الهيئات المهنية والتشريعات والادلة الاجنبية والعربية فضلا عن الاستراتيجيات الوطنية (ما قدم من قبل *(AICPA)*والدليل الارشادي ل *(SEC)*والارشادات الرقابية المالية لبورصة تورنتو *(TSX)* والمؤشر المقدم من قبل شركة ارنست ويونغ *(E8Y)* ونموذج (10 *(k-*للشركات *fortune100* و معيار مجلس معايير الاستدامة *(SASB*)

الكلمات المفتاحية: الإفصاح السيبراني، مخاطر الامن السيبراني، مؤشر سيبراني

Abstract

The research aims to propose an indicator for the disclosure of cyber risks within the information disclosed in the annual reports issued by economic units and due to the absence of instructions regulating this type of disclosure within the disclosure instructions within the disclosure instructions No. (8) for the year (2015) amended for the Iraq Stock Exchange and given the decline of Iraq's position in the global cyber security index issued by the United Nations specialized agency in information and communications technology according to the (GCI) index, where Iraq achieved 129th position globally out of (184) despite the increasing interest of the Iraqi state in developing a cyber-security strategy (2018) Accordingly, an indicator for accounting disclosure of cyber security risks has been built in accordance with international requirements issued by professional bodies, foreign and Arab legislation and evidence, as well as national strategies (provided by (AICPA), the SEC guideline) and the financial control guidelines of the Toronto Stock Exchange (TSX). The index provided by Ernst & Young (E8Y), the fortune100 (10-k) model, the Sustainability Standards Board (SASB) FN-CB standard.

Keywords : Cyber disclosure, cyber security risks, cyber index.

*المؤلف المراسل

1.مقدمة:

مع توسع الأسواق عالميا وتعقدها تزداد التهديدات من خلال التطفل السيبراني ((cyber intrusion والهجمات السيبرانية. وغيره من سوء التفاعل السيبراني وفي عالم اليوم المتصل رقميا. تعد المخاطر السيبرانية تهديدا مستمرا ومتصاعدا على الشركات وأصحاب المصالح (المستثمرين، المقرضين .....). زادت بالآونة الأخيرة هذه المخاطر بحكم رقمنه المعاملات نتيجة حدوث جائحة covid 19 وقدرة مخترقي شبكة المعلومات من تحقيق دخل مرتفع من حوادث الامن السيبراني من خلال برامج عدة، فضلا عن استخدام الأصول المشفرة ((crypto-assets ونمو المدفوعات الرقمية وازياد اعتماد الوحدات الاقتصادية على مزودي خدمات التكنولوجيا والمعلومات بما في ذلك تكنولوجيا الحوسبة السحابية. وقدمت الهيئات المحاسبية المهنية العديد من متطلبات الإفصاح كما هو الحال مع اللوائح المقدمة من قبل SEC,AICPA وغيرها.

وفي ضوء ازدياد هذه المخاطر من خلال الهجمات السيبرانية تحاول الهيئات المهنية وضع اطر وارشادات لتنظيم عملية الإفصاح عن تلك المخاطر ومنها (SEC,AICPA,ICEW)، وتضمنت منهجية البحث الاتي: -

1.1 مشكلة البحث:

مع ازدياد المخاطر السيبرانية في العالم عموما وفي العراق باعتباره جزء من المنظومة الرقمية العالمية بحكم التعاملات مع دول العالم خصوصا في القطاع المصرفي .و باستقراء ارض الواقع بخصوص الافصاح في السوق المالية العراقية بتقارير عن مخاطر الامن السيبراني يلاحظ افتقار تعليمات الإفصاح في سوق العراق للأوراق المالية رقم 8 لسنة 2015 المعدل –عن تعليمات صريحة بخصوص هكذا نوع من التقارير فضلا عن غياب لمؤشر يختص بالإفصاح عن المخاطر السيبرانية لكافة القطاعات المدرجة في السوق وغياب المتطلبات الإلزامية او الطوعية للإفصاح عن هكذا نوع من التقارير الاضافية وعلى وفق ذلك تثار الأسئلة البحثية الاتية:

- هل بالإمكان بناء مؤشر للإفصاح عن المخاطر السيبرانية في البيئة العراقية.
- هل تفصح الشركات (عينة البحث) عن المخاطر السيبرانية على وفق فقرات المؤشر المقترح.

2.1 أهمية البحث:

تنبع أهمية البحث من أهمية المخاطر السيبرانية التي ازدادت في الآونة الأخيرة بحكم ازدياد تطور تكنولوجيا المعلومات والاتصالات والتحولات الرقمية ومحاولة تأطير الإصدارات المهنية الخاصة

بالإفصاح عن المخاطر السيبرانية والاستعانة بها في محاولة للحد من هذا المخاطر في أحد القطاعات المهمة وهو القطاع المصرفي العراقي.

3.1 اهداف البحث:

يهدف البحث الى محاولة بناء مؤشر للإفصاح المحاسبي عن المخاطر السيبراني في سوق العراق للأوراق المالية واستعراض التطورات التي طرأت على الإفصاح عن هذه المخاطر وفق الإصدارات المهنية المحاسبية مع استعراض الاستراتيجيات للعديد من الدول في التعامل مع الامن السيبراني.

4.1 فرضية البحث: يركز البحث على فرضية رئيسية مفادها.

الفرضية الأولى" بالإمكان بناء مؤشر للإفصاح عن امن المخاطر السيبراني في سوق العراق للأوراق المالية.

الفرضية الثاني" هناك تباين في الإفصاح عن مخاطر الامن السيبراني في المصارف العراقية المدرجة في سوق العراق للأوراق المالية.

5,1 مجتمع وعينة البحث:

يتمثل مجتمع البحث بالمصارف المدرجة في سوق العراق للأوراق المالية للفترة (2019-2020) وعددها 38 مصرف في حين يمثل عينة البحث المصارف التي تتعامل وبكثافة بالأنشطة السيبرانية وتم اختيار أربع مصارف مدرجة في السوق وهي مصرف بغداد التجاري ومصرف الخليج التجاري ومصرف الاهلي التجاري ومصرف العراقي التجاري.

2. دراسات سابقة واسهامه البحث الحالي

1.2 دراسات سابقة

تناولت الدراسات المخاطر السيبرانية والافصاح عنها في التقارير المالية في العديد من الدراسات العراقية والأجنبية وكالاتي:- :

١-دراسة (الرشيدي وعباس،2019) بعنوان إثر الإفصاح عن مخاطر الامن السيبراني في التقارير المالية على أسعار الأسهم وحجم التداول المصرية.

بحث منشور في مجلة المحاسبة والمراجعة.

يهدف البحث الى التعرف على طبيعة الإفصاح عن المخاطر الامن السيبراني في التقارير المالية وعن برنامج إدارة المخاطر في الشركات المصرية وأثر ذلك على أسعار الأسهم وتوصلت الدراسة من خلال الاستعانة بالاستبانة كأحد ادوات البحث العلمي الى ضعف الإفصاح عن مخاطر الامن السيبراني وبرامج إدارة مخاطره في الشركات المصرية المدرجة في السوق المالي المصري .

٢ –دراسة (علي وعلي،2022) بعنوان (إثر الإفصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. (دراسة تجريبية) بحث منشور في وقائع مؤتمر جامعة الإسكندرية

يهدف البحث الى دراسة واختبار إثر الإفصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية من خلال اجراء دراسة تجريبية على عينة من المستثمرين بالأسهم والمحللين الماليين في شركات السمسرة وتوصلت الدراسة الى وجود تأثير إيجابي ومعنوي لتقرير إدارة مخاطر الامن السيبراني على قرار الاستثمار في الشركات.

3 –دراسة (صالح ،2022) بعنوان (محددات فعالية المراجعة الداخلية للأمن السيبراني)

يهدف البحث الى استكشاف الاجراءات الناجعة لتحديد فاعلية التدقيق للأمن السيبراني والعوامل المؤثرة على ذلك، من خلال الاعتماد على الدراسة التحليلية لاهم الاصدارات المهنية بهذا المجال وتوصل البحث الى امكانية تحديد العوامل المؤثرة في فاعلية التدقيق للشركات في ظل الامن السيبراني.

4–دراسة (Fortin &Herou 2020– بعنوان Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index)

الإفصاح عن الامن السيبراني في الشركات على وفق مؤشر.S&P/TSX 60

تهدف الدراسة اختبار مدى الإفصاح عن المخاطر السيبرانية في تقرير تعليقات الإدارة للشركات التي تضم مؤشر S&P/TSX 60 وهل هذه الافصاحات متوافقة مع الممارسات الدولية المهنية في الإفصاح عن المخاطر، وتوصل البحث الى ان الشركات بقطاعاتها المختلفة إفصاحات عن مخاطر الامن السيبراني في تقرير تعليقات الإدارة الا انه بشكل عام كان هناك انخفاض في الافصاح للفترة (2017–2018) واوصى البحث بتطبيق معايير اكثر صرامة في الاسواق المالية بخصوص الافصاح عن الامن السيبراني.

4 –دراسة (Ramirez et.al.2022)

The disclosures of information on sybersecurity in listed companies in Latin America– proposal for syber security disclosure index

يهدف البحث الى بناء مؤشر للإفصاح عن المخاطر السيبرانية للشركات في امريكا اللاتينية وتم بناء المؤشر من 30 فقرة

2.2 اسهامة البحث الحالي

وتأسيسا لما تقدم فان البحث الحالي يتميز باسهامته البحثية المتمثلة ببناء مؤشر مقترح للإفصاح عن المخاطر السيبرانية مرتكزا على ما قدمته الهيئات المهنية والخطط الاستراتيجية للمخاطر السيبرانية.

3. أدارة مخاطر الامن السيبراني: مدخل تعريفي

1.3 المخاطر السيبرانية –المفهوم:

مخاطر الامن السيبراني (Cybersecurity risk) هي 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 فقد عرفها (NIST) المعهد الوطني للمعايير والتقنية بأنها عملية حماية المعلومات عن طريق منع الهجمات من خلال كشفها والتصدي لها (INIST) وعرفتها (ISO) المنظمة الدولية لمعايير الجودة بأنه الفضاء الذي يتمثل في الحفاظ على السرية والسلامة وتوافر المعلومات في الفضاء السيبراني ويعرف (بانه البيئة الناتجة عن تفاعل الافراد مع البرمجيات والخدمات المتاحة من خلال الانترنيت عن طريق الأجهزة والتقنيات والشبكات المتصلة به وليس لها وجود فيزيائي (الدليل الاسترشادي للأمن السيبراني لمؤشرات السوق المالية السعودي، ٢٠١٨.)

وباتجاه اخر فأن مخاطر الامن السيبراني ((Cybersecurity risk من اهم المخاطر التي تواجه الشركات، فهي المخاطر التي يمكن ان تواجه الشركات بما فيها رسالة الشركة ورؤيتها او (لوغو) شعارها او سمعتها او صورها بسبب إمكانية الوصول غير المصرح او سوء الاستخدام او تدمير المعلومات (الهيئة المصرية للأمن السيبراني المصري، ٢٠١٨،١١٦.)

وعرفتها الاستراتيجية الوطنية للأمن السيبراني في العراق بانها احتمال وجود تهديد وهشاشة داخل الفضاء الالكتروني للبلد يضر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية من خلال التهديدات السيبرانية والثغرات الموجود في الفضاءات السحابية (استراتيجية الامن السيبراني العراقية، 6،٢٠٢٠) وبنفس الاتجاه عرفها القانون الامن السيبراني الأردني رقم ١٦ لسنة ٢٠١٩،

وتلعب المحاسبة والتدقيق دورا مهما في إدارة مخاطر الامن السيبراني على اعتبار انها من المخاطر الناشئة وهي الخطر الذي يؤدي الى خسائر مالية فادحة فضلا عن مخاطر السمعة والمخاطر التشغيلية، من خلال بناء إدارة فاعلة لمخاطر الامن السيبراني (مشابه لنظام الرقابة الداخلية) بأجراء الاختبارات اللازمة لفاعلية عناصر رقابة الامن السيبراني باختيار نقط مرجعية معيارية(لضوابط التكنولوجيا) داخل الوحدة الاقتصادية ، ويتم ذلك من خدمات التوكيد وخدمات الاستشارية في مجالات تكنولوجيا المعلومة حيث تلعب خدمات التوكيد المقدمة من قبل مراقب الحسابات كخدمات أخرى دورا في توكيد فاعلية البرنامج المعتمد في إدارة مخاطر الامن السيبراني في الوحدة الاقتصادية فضلا عن الإفصاح الطوعي او الالزامي عن مخاطر الامن السيبراني وفقا للأدلة والاطر الاسترشادية المقدمة في الهيئات المهنية او الهيئات المنظمة للأسواق المالية كتقرير الامن السيبراني للمعهد الأمريكي للمحاسبين القانونيين AICPA وتقرير الامن السيبراني الصادر عن لجنة تبادل الأوراق المالية في البورصة الامريكيةSEC ، (kemiyaetal,2018:3) (Eaton,2019,3) ، (الرشيدي، ٢٠١٩:٤٦٦). وتأسيسا لما تقدم فان مخاطر السيبرانية تشكل أحد المخاطر المستحدثة في البيئة العالمية والمحلية وان الوحدات الاقتصادية بحاجة الى الافصاح عن المخاطر التي جابهتها أو التي يتوقع ان تجابهها لتعزيز الافصاح والشفافية في تقاريرها السنوية.

2.3 الهيئات المهنية المحاسبية والمخاطر السيبرانية:

زادت الاهتمام من قبل الهيئات والمجاميع المهنية المحاسبية والمنظمة للإفصاح في الأسواق المالية حول مخاطر الامن السيبرانية خاصة بعد التهديدات والخروقات الكبيرة التي تعرض لها شركات القطاع المصرفي والشركات بكافة قطاعاتها وعلى وفق ذلك اصدرت العديد من الهيئات طروحاتها بهذا الخصوص وكالآتي: -

1- لجنة تبادل الأوراق المالية الامريكية Securities and exchange (SEC) commission

اصدرت دليل استرشادي بمتطلبات الإفصاح عن الامن السيبراني ومخاطره عام ٢٠١٨. سبقته دليل لعام ٢٠١١ (SEC) بعنوان (statement on PROPOSAL mandatory cyber security disclosure)وتقترح ال (SEC) بغرض الإفصاح الالزامي فعلى الشركات ان تفصح بتقرير منفصل او مدمج مع تقارير الشركة وتقترح ان تكون مع تقرير تعليقات الإدارة

وترى ان هذا الإفصاح سيعزز في قدرة المستثمرين على تقييم ممارسات الامن السيبراني للشركات والابلاغ عن الحوادث السيبرانية والاختراقات بحكم انها فرصة لجعل المستثمرين يقرروا عن أي مخاطر التي يرغبون بتحملها واعتبرت (SEC) المخاطر السيبرانية من المخاطر الناشئة ولها تأثيرات مالية وتشغيلية وقانونية والحاجة الى تقارير عم الاحداث الجوهرية للمخاطر السيبرانية وقدمت (SEC) النموذج (k-8) 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 الإجراءات المتبعة من قبل الإدارة للإفصاح عن مخاطرها واداراتها للأمن السيبراني واقترح (، SECفي عام 2022 بعض التعديلات المقدمة في الإبلاغ المالي عن حوادث الامن السيبراني الجوهرية والتقارير الدورية لتقديم تحديثات حول حوادث الامن السيبراني التي يتم الإبلاغ عنها اذ تقترح (SEC) تقارير دورية حول سياسات وإجراءات الشركة 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 إفصاحات الامن السيبراني في لغة الاعمال (XBRL) وارفقت (SEC) هذه الافصاحات بقاعدة تشريعية قانونية متمثلة بقانون الأوراق لمخاطر وحوادث الامن السيبراني الأمريكي ٢٠١١، فضلا عن إرشادات الإفصاح CF-13 الامن السيبراني الصادر في 13 تشرين الاول ،2011 متاح على الموقع:

www.sec.govldivisions /Corpfin/guidance/cfguidance.topic.htm

والارشادات حول افصاح الامن السيبرانية رقم 33. 10459 في 26 نيسان 2018(speeches of gensler president chair the us. secuputies and exchange commission ,2022,1-16)

٢- المعهد الأمريكي للمحاسبين القانونيين American institute of certified public accountants ((AICPA

قدم دليلا للإفصاح الاختياري عن المخاطر السيبرانية في ٢٦ نيسان ٢٠١٧ من خلال اصدار معايير لوصف الأسلوب الذي من خلاله يتم تبني سياسات وإجراءات احترازية للوصول الى

إدارة مخاطر امن سيبرانية فاعلة والافصاح عن المؤشرات التي تمكن مستخدمي معلومات تقرير مخاطر الامن السيبراني من فهم المخاطر والأسلوب التي يتم ادارته بها ويساعد الاطار المقدم من قبل AICPA)) في تحديد خطوات اعداد تقارير إدارة مخاطر الامن السيبراني فضلا عن خدمات التدقيق المرافقة له، وحددت AICPA)) التقرير التي تلتزم به الشركات (طوعيا) للإفصاح عن مخاطر الامن السيبراني ويوضح الشكل (١) الجزء الأول من تقرير الإفصاح عن مخاطر الامن السيبراني المقدم من قبل AICPA.

الشكل 1: القسم الأول من تقرير الإفصاح عن مخاطر الامن السيبراني وفقاً لـ (AICPA)

أول
managemer
ادارة

وصف نوعي يعد من قبل الإدارة يتعلق بماهية برامج إدارة مخاطر الامن السيبراني المعتمد في الوحدة الاقتصادية على وفق المعايير المعدة مسبقا من قبل AICPA و التي تشمل:

١-معايير الوصف ويتضمن: -ماهية الشركة وطبيعتها

-أنواع المعلومات الواجب الإفصاح عنها وتجميعها لدى الشركة Descriptions criteria

-اهداف برامج إدارة مخاطر الامن السيبراني

- هيكل حوكمة إدارة مخاطر الامن السيبراني
- تحديد المخاطر الالكترونية المؤثرة على ادارة امن المخاطر السيبراني
- جودة الامن السيبراني
- أنشطة مراقبة الامن السيبراني وتقييم جودتها
- توصيل المعلومات الى الأطراف المختلفة

المصدر: اعداد الباحثون وفق متطلبات AICPA للإفصاح عن مخاطر الامن السيبراني ٢٠١٧ ويتكون القسم الثاني والثالث من تقرير الإفصاح عن مخاطر الامن السيبراني على وفق AICPA /٢٠١٧ من قسمي توكيد الإدارة ورأي مراقب الحسابات وكما بالجدول رقم (1).

الجدول 1: تقرير الإفصاح عن مخاطر الامن السيبراني

القسم الثاني	القسم الثالث
توكيد الإدارةmanagement description –توكيد إدارة الوحدة الاقتصادية بان التقرير قد تم اعداده وفق متطلباتAICPA ، وان ضوابط الرقابة كانت على وفق إدارة مخاطر الامن السيبراني	راي الممارسين The practitioners opinion ويتضمن تدقيق تقرير إدارة مخاطر الامن السيبراني المعد من قبل إدارة الوحدة الاقتصادية، وان قد تم الحصول على ادلة اثبات كافية وعلى وفقها تم بلورة رأي مراقب الحسابات بشأن التقرير.

المصدر: اعداد الباحثون على وفق متطلبات (AICPA) ٢٠١٧

3- اهتم معهد المحاسبين القانونين الكندي (CPA.CANDA) (CPA) وبنفس السياق وبالتعاون مع هيئة سوق الأوراق المالية الكندية Canadian sweeties) (administratorsقدمت دليل ارشادي للشركات المدرجة في سوق الأوراق المالية الكندية عن أسلوب الإفصاح عن مخاطر الامن السيبراني عام ٢٠١٧ وأوضحت الهيئة المكان التي يتم به عرض تقرير امن مخاطر السيبرانية وذلك في تقرير تعليقات الإدارة مع إضافة بند لتحليلات الإدارة تأثيرات المخاطر السيبرانية على نشاطات الوحدة الاقتصادية المالية والتوقعات المستقبلية) ٤٩-١-٢٠١٧.(SPA-

4- مجلس معايير الاستدامة SASB)) وقد تضمن معيار (FN-CB) الصادر عن المجلس فقرات تتعلق بالأمن السيبراني(www.sasb.org) والخاص بالمصارف التجارية ويتضمن المعيار المؤشرات الآتية- :

أ) عدد الخروقات السيبرانية خلال فترة معينة .

ب) النسبة المئوية التي تتضمن معلومات تعريف شخصية (معلومات تحديد الهوية الشخصية)

ج) نسبة الحسابات المصرفية المتأثرة بالهجمات السيبرانية

د) وصف لا دارة مخاطر الامن السيبراني.

5- بورصة تورنتو (TSX) قدمت بورصة تورنتو مؤشرا للإفصاح عن مخاطر الامن السيبراني من اربعين فقرة موزعة في سبع فئات فضلا عن مشاركة شركة ارنست ويونغ تقريرا للإفساح يتكون من ابعاد عدة منها اشراف مجلس الادارة ومستوى مجلس الادارة واعداد تقارير الادارة والابلاغ عن ادارة مخاطر وجهود الادارة لتخفيض المخاطر السيبرانية والتعليم والتدريب

وبنفس السياق اهتمت الهيئة المهنية العربية بإصدار ادلة ارشادية او استراتيجيات حول المخاطر السيبرانية ونستعرض بعض من هذه الإصدارات:

1 - دليل هيئة سوق المال السعودي ٢٠١٩ حيث أصدر هيئة سوق المال السعودي ٢٠١٩ دليلا ارشاديا للأمن السيبراني يختص بالمؤسسات المالية، ويحدد الضوابط المتعلقة بالأمن السيبراني للشركات السعودية المدرجة في السوق السعودي المالي. فضلا عن اصدار الهيئة الوطنية للأمن السيبراني الضوابط الأساسية للأمن السيبراني ٢٠١٨ ECC-1-

2- دليل البنك المركزي الأردني ٢٠١٨ حيث أصدر البنك المركزي الأردني ادلة استرشادية للتعامل مع مخاطر الامن السيبراني والسبل الكفيلة بمواجهة الهجمات السيبرانية وفق الدليل رقم ٦ لسنة ٢٠١٩ حيث اعتبر مخاطر الامن السيبراني بأنها الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الامن السيبراني والقدرة على استعادة عملها واستمرارها سواء اكان الوصول اليها بدون تصريح او سوء استخدام او نتيجة الإخفاقات في اتباع الإجراءات الأمنية او التعرض للخداع الذي يؤدي الى ذلك (قانون الامن السيبراني الأردني،٢٠١٩).

3- مصر / أصدرت مصر الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١) تتضمن الاستراتيجية عددا من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبراني .

4- العراق/ الاستراتيجية الوطنية للأمن السيبراني هي استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به عادة، تتألف استراتيجية الامن السيبراني الوطنية من عدة استراتيجيات قصيرة ومتوسطة وطويلة الأمد (الاستراتيجية الوطنية للأمن السيبراني .2018) ويرى الباحثون انها استراتيجيه عامة تعزز من الامن السيبراني في البيئة العراقية الا انها تعمل بشكل شمولي لكافة القطاعات ولم تعط الخصوصية لاي قطاع من القطاعات.

3.3 الإفصاح المحاسبي عن مخاطر الامن السيبراني:

يعد الإفصاح المحاسبي عن مخاطر الامن السيبراني من المجالات البحثية التي نالت حيزا واسعا حيث بينت دراسة .(Liatel.2018.30) ان الوحدات الاقتصادية تعمل على الإفصاح عن مخاطر الامن السيبراني من خلال تقرير تعليقات الإدارة بشكل وصفي لإعطاء إشارات إيجابية لأصحاب المصالح ان الوحدة الاقتصادية قد أسهمت في إدارة المخاطر السيبرانية وأنها افصحت عن جهودها في ذلك من خلال الإفصاح النوعي في أحد تقارير الوحدة الاقتصادية. وبالتالي تعطي صورة مشرقة عن الوحدة الاقتصادية بانها كانت استباقية في حفاظها على امن المعلومات وتقليل حالات الهجمات السيبرانية عليها. وان الإفصاح عن تقرير إدارة مخاطر الامن السيبراني يرسل إشارات إيجابية عن الوحدة الاقتصادية كفئة المستثمرين مثلا وبقية أصحاب المصالح حول الجهود المبذولة في مجال الامن السيبراني والحماية من الهجمات الالكترونية وبالتالي يساهم في الحد من ظاهرة عدم تماثل المعلومات بين الإدارة وأصحاب المصالح مما يمكن المستثمرين من تقييم قدرة الوحدة الاقتصادية من الحفاظ على امن المعلومات وتقليل احتمالات حدوث اختراقات واحداث سلبية في المستقبل، مما يساعد على تحسين كفاءة قرارات المستثمر التي يتم اتخاذها في توفير الثقة في اعمال الوحدة ويتعكس إيجابا على تحسن الأداء المالي للشركة (علي وعلي،12،٢٠٢٢) فضلا عن ان الافصاحات (الطوعية) تمثل احد اهم المتطلبات التي ازدادت الدعوات لها من قبل الهيئات المهنية والاطر المحاسبية الفكرية نحو التوسع في الإفصاح المحاسبي. لخدمة أصحاب المصالح ومنها المستثمرين، فالإفصاح عن المخاطر الأمنية السيبرانية يسهم في اتجاه التأثير الإيجابي على قرارات المستثمرين حتى وان لم يكن المستثمر (حصيف)(yangeted.,2020,167) ،وقد يسهم في اتجاه ثقة أصحاب المصالح ومنهم المستثمرين بالوحدة الاقتصادية وينعكس على جودة القرار المتخذ في ظل الصناعات التي تعاني من هجمات سيبرانية شرسة ويعزز من جاذبية المستثمرين (Kelton&pennington,2020)ويوضح(الرشيدي والسيد) بأن الإفصاح في القوائم المالية يتأثر بحوادث الامن السيبراني والمخاطر الناتجة منها على القوائم المالية للشركة حيث يمكن ان تؤدي الى: (الرشيدي وعباس،٤٦٢،٢٠١٩)-:

١-زيادة زيادة المصروفات المتعلقة بالتحقيق والاخطار بالاختراق وكيفية علاج ذلك وإمكانية التقاضي وبما يرتبط بها من تكاليف الخدمات القانونية وغيرها من الخدمات المهنية الأخرى.

٢-انخفاض الإيرادات حيث يتعين اما تقديم مزيد من الحوافز (للزبائن) للحفاظ عليهم والا يتم خسارتهم.

٣-المطالبات المتعلقة بالضمانات وعدم الوفاء بالعقد واسترجاع المنتج والتعويضات للأطراف.

٤-انخفاض التدفقات النقدية المستقبلية او اضمحلال الأصول الفكرية او غير الملموسة وغيرها من الأصول فضلا عن الاعتراف بمزيد من الالتزامات وزيادة تكاليف التحويل.

وينعكس ذلك على تصميم نظم التقرير المالي ونظم الرقابة لها لتوفير ضمان معقول بان المعلومات الخاصة بنطاق وحجم التأثيرات المالية لحوادث الامن السيبراني تم اخذها بعين الاعتبار عن اعداد القوائم المالية في الوقت المناسب عندما تصبح المعلومات متاحة.

وتأسيسا لما تقدم فان استجابة الوحدات الاقتصادية للإفصاح عن مخاطر الامن السيبراني يعد الركيزة الاساس للمحافظة على الثقة ومصداقية التقارير المرافقة للتقارير المالية والمتعلقة بالإفصاح عن مخاطر الامن السيبراني التي توليها الجهات المحاسبية والرقابية الاهتمام المتزايد، دوريا(سنويا)

4.3 مخاطر الامن السيبراني في القطاع المصرفي:

لا تتعرض كل الصناعات بشكل متطابق للمخاطر السيبرانية. ووفقاً لسيناريوهات تراكم المخاطر risk accumulation scenariosالتي طورتها سويس ري Swiss Re ، فإن القطاع المصرفي هو الأكثر تعرضاً للتهديدات ، يليه المراكز الطبية ثم قطاع التأمين ،وتتمثل المخاطر السيبرانية في القطاع المالي بالتالي (نشرة الاتحاد المصري للتأمين ،2019 ،3-17)-:

1-سرقة أو فقدان البياناتTheft or Loss of Data

البيانات الشخصية والبيانات التجارية، وأي بيانات ذات قيمة بالسوق السوداء تعتبر خطر.

الدافع: المكاسب المالية أو التنافسية.

2-تدميرالبياناتData Destruction

مسح البيانات الالكترونية أو تشفيرها أو منع الوصول اليها.

الدافع: والابتزاز، والإرهاب، أو الحرب.

3-انقطاع الاتصالاتCommunication Disruptions

تعطيل الموقع الالكتروني أو تعطيل الشبكة؛ تشويه الموقع؛ الاستيلاء على صفحات وسائل التواصل الاجتماعي.

الدافع: الإيديولوجية، والابتزاز، والإرهاب، أو الحرب.

5- سرقة الأموال والأوراق المالية والصناديق وغيرها ,Theft of Monies, Securities Funds, etc

ما وراء سرقة البيانات: المال والأوراق المالية هي هدف عالي القيمة سواء مادياً وإلكترونيا.

الدافع: المال.

ففي شباط ومن عام ٢٠١٦ استهدف مخترقو الأنظمة السيبرانية في البنك المركزي البنغلاديش واستغلوا نقاط الضعف في (swift) وهو نظام رسائل الدفع الالكتروني الرئيسي للنظام المالي العالمي وحقق هذا الهجوم السيبراني خسارة ما يقرب الملیار دولار وكانت هذه السرقة بمثابة جرس انذار لعالم المال بان المخاطر السيبرانية في النظام المالي ازدادت في ظل التكنولوجيا المالية المطبقة في المصارف، وحذر مجلس الاستقرار المالي (financial stability boards) ان أي حادث اختراق سيبراني يعمل على تعطيل الأنظمة المالية بشكل خطير ويوقف البنية التحتية المالية ويؤدي الى تداعيات أوسع على الاستقرار المالي ويؤدي الى تكاليف اقتصادية هائلة فضلا عن انفاقها على انخفاض ثقة الجمهور بالقطاع المصرفي transactional monetary fund, 2021,).و بنفس السياق عانى مصرف كابيتال من الاختراق السيبراني وتكبد خسارة نتيجة سرقة بيانات (١٠٦) ملايين زبون امريكي وكندي من زبائن مصرف كابيتال وان الأمريكي وتعرض المصرف الى قرصنة معلوماتية وهي اكبر عمليات القرصنة لخامس مصدر لبطاقات الائتمان المصرفية في أمريكا وتم استغلال ثغرة في (cloud) الخادم المعلوماتي الافتراضي للمصرف وقد دفع المصرف غرامة قدرها (٨٠) مليون دولار للجهات التنظيمية الامريكية بسبب حادث القرصنة وقد اتخذ المصرف خطوات لتشديد الامن حول معلومات الزبائن وتعرضت خوادم المصارف الاوربية للاختراق في الهجوم الالكتروني على شركة مايكروسوفت:

أعلن الاتحاد الأوربي ٢٠١٩ ان خوادم البريد الالكتروني التابع للسلطة المصرفية الاوربية (European banking authority)تعرض للاختراق في الهجوم الالكتروني الذي تعرض له.

وحاولت الشركات بمختلف السبل من تعزيز الافصاح عن المخاطر السيبراني في تقاريرها السنوية بتضمين التحليلات والإفصاحات الملائمة في تقرير تعليقات الادارة او بتقارير اضافية. وفي تقرير لمجلة

(fortune) لأفضل ١٠٠ شركة ضمن قائمة ٥٠٠ شركة أمريكية لتحديد اتجاهات تطور الإفصاح عن مخاطر الامن السيبراني، حيث تم اختيار افصاح (٧٦) شركة ضمن قائمة (fortune) للفترة بين (٢٠١٨-٢٠٢٠) حيث تمثل (10-k)التقارير السنوية وتقارير (Q-10) الربع سنوية (اما إذا دعت الحاجة الى استخدام النموذج (8 (K-وذلك عند توفر اخطار معلومات جوهرية متعلقة بالأمن السيبراني وإذا احتاج الامر الى الإفصاح الفوري عن المخاطر فانه يتم الاعتماد على انموذج (6 (K-حيث حددت (SEC) تلك النماذج وفق اطرها المعلنة. ويوضح جدول (2) إفصاحات مخاطر الامن السيبراني لأفضل ١٠٠ شركة أمريكية نشرتها مجلةfortune

الجدول 2: إفصاحات مخاطر الامن السيبراني لأفضل ١٠٠ شركة أمريكية نشرتها مجلة fortune

الفقرة	الإفصاح	٢٠١٨	٢٠١٩	٢٠٢٠
مدخل مراقبة المخاطر	التركيز على الامن السيبراني في قسم مراقبة المخاطر في تقرير تعليقات الإدارة.	٪*٧٩	٪٨٨	٪٨٩
الاشراف على لجنة المخاطر من قبل مجلس الادارة	الإفصاح عن تكليف لجنة واحدة على الأقل على مستوى مجلس الإدارة بالأشراف على شؤون الامن السيبراني.	٪٧٤	٪٨٢	٪٨٧
	. الإفصاح على ان لجنة التدقيق تشرف على مسائل الامن السيبراني	٪٥٩	٪٦٢	٪٦٧
	الاشراف على مخاطر الامن السيبرانية من لجنة ليست لجنة تدقيق وانما لجنة فنية.	٪٢٠	٪٢٨	٪٢٦
هيكل تقرير الادارة	يتوافق مع الرؤى المقدمة من الهيئات المهنية وبرؤى خاصة للشركة نفسها.	٪٥٤	٪٥٨	٪٦١
تكرار التقرير	تقديم تقارير الى مجلس الإدارة بشكل غير منتظم وغير مكرر.	٪٣٨	٪٤٥	٪٤٧
	تقرير يتم الإفصاح عنه بمعدل سنوي او ربع سنوي على الأقل واستخدمت الشركات مصطلحات دوريا او بانتظام.	٪١٤	٪١٧	٪١٧
قائمة مخاطر الامن السيبراني	الإفصاح عن عوامل الخطر وسرية المعلومات.	٪١٠٠	٪١٠٠	٪١٠٠

جهود إدارة مخاطر الامن السيبراني	الإفصاح عن الجهود لخفض مخاطر الامن السيبراني (انشاء لعمليات والإجراءات الاحترازية) والمحاكاة وغيرها.	٨٣٪	٩١٪	٩٢٪
التعليم والتدريب	الإفصاح عن الجهود لتعليم والتدريب للتخفيف من مخاطر الامن السيبراني.	١٨٪	٢٦٪	٢٩٪
المشاركة مع المجتمع الخارجي	الإفصاح عن التعاون مع الجهات الخارجية لتخفيف مخاطر الهجمات السيبرانية.	٧٪	١٢٪	١٢٪
توظيف مستشار خارجي مستقل	الإفصاح عن توظيف مستشار خارجي مستقل.	٣٪	٤٪	٥٪

المصدر: عداد الباحثون

***النسب المئوية على أساس اجمالي الافصاحات للشركات. تستند البيانات الى (٧٦) شركة مدرجة في**
قائمة (fortune–100) لعام ٢٠٢٠ والتي قدمت إفصاحات على وفق النموذج (k–10) وللفترة من (٢٠١٨–٢٠٢٠).

رابعا–الدول العربية: في المؤشر العالمي للأمن السيبراني الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات (الاتحاد الدولي للاتصالات).

المؤشر العالمي للأمن السيبراني يتضمن محاور (المحور القانوني والمحور التقني والمحور التنظيمي ومحور بناء القدرات ومحور التعاون) ويتم تحليل أداء الدول على وفق هذا من قبل فريق (GCI)من خلال (٨٠) مؤشرا فرعيا لغرض تحقيق اعلى مستوى من الامن السيبراني وتعزيز تبادل الخبرات ومشاركة تجارب العالم.
وحققت بعض الدول مراكز متقدمة في هذا المؤشر حيث حققت السعودية المركز ٤٦ عالميا من بين ١٩٣ دولة. ويتكون التقييم للدولة على وفق مدى التزام الدولة بالفقرات المعلن عنها وفق المحاور والذي يتم بمسح جميع البيانات المتعلقة بالدولة من اجل الوصول الى مجموع نقاط المؤشر.

وقد حقق العراق من خلال مؤشر (GCI) عام ٢٠١٨ المركز (١٠٧) عالميا و(١٣) عربيا وقد تراجع (٢٢) نقطة في مؤشر العام (٢٠٢٠) ليكون (١٢٩) عالميا من أصل (١٨٤) دولة و(١٧) عربيا بدرجة (٧١،٢٠)، ويوضح الجدول (3) اهم الفقرات المتعلقة بمؤشر (GCI) الخاص بمركز العراق في الامن السيبراني:

الجدول 3: الفقرات المتعلقة بمؤشر (GCI) الخاص بمركز العراق في الامن السيبراني

الإجراءات القانونية	الإجراءات التقنية	الإجراءات التنظيمية	بناء القدرات	التعاون	المجموع الكلي
0.00	6.56	7.75	2.14	4.6	20.7

المصدر: (Global cyber security index).

4. تحليل النتائج

1.4 بناء مؤشر للإفصاح عن مخاطر الامن السيبراني CRI مع حالة تطبيقية

لغرض تحقيق بناء مؤشر للإفصاح عن مخاطر الامن السيبراني ستتم الاستعانة بما اصدرته الهيئات المهنية والتشريعات والادلة الاجنبية والعربية فضلا عن الاستراتيجيات الوطنية (ما قدم من قبل (AICPA) والدليل الارشادي ل(SEC) والارشادات الرقابية المالية لبورصة تورنتو (TSX) والمؤشر المقدم من قبل شركة ارنست ويونغ (E8Y) ونموذج (k–10) للشركات fortune100 و معيار مجلس معايير الاستدامة ((SASB وقد تضمن معيار (FN–CB) بعض المؤشرات الخاصة بالأمن السيبراني فضلا عن الاستعانة باستراتيجيات الامن السيبراني العراقي 2018.

اولا: الوضع التنظيمي للمؤشر المقترح

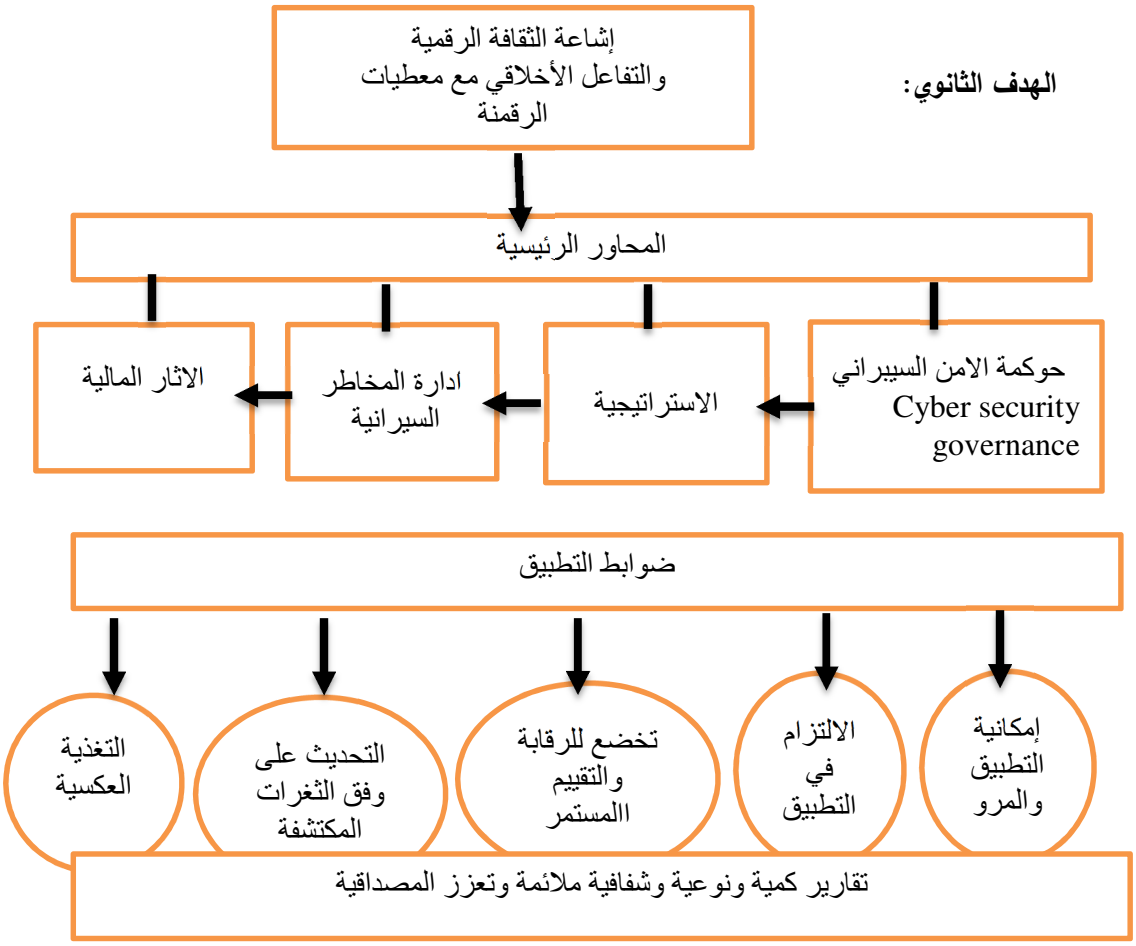
يتكون المؤشر المقترح من ابعاد (خمس) وهي الحوكمة السيبرانية، الاستراتيجية، ادارة المخاطر السيبرانية والاثار المالية، ويوضح الشكل (2) اهم الابعاد الرئيسية والهدف من بناء مؤشر للإفصاح عن مخاطر الامن السيبراني.

الشكل 2: الابعاد الرئيسية واهداف المؤشر المقترح لمخاطر الامن السيبراني.

الهدف الرئيسي:

توفير أدنى حد ممكن من المتطلبات الرئيسية للأمن السيبراني للمعاملات في الشركات المدرجة في السوق المال

الهدف الثانوي:



المصدر: اعداد الباحثون

-المصطلحات المرافقة للمؤشر: لابد من تأطير المؤشر المقترح بالتعاريف الساندة لضمان سهولة ومرونة تطبيق المؤشر

1-الحوكمة السيبرانية ٢-الثغرات٣-مخاطر الامن السيبراني

1-حوكمة الامن السيبراني حوكمة الامن السيبراني على وفق معيار ISO / IEC 2

هي النظام الذي توجه وتتحكم به الوحدة الاقتصادية من خلال ادارة الامن ويحدد إطار المسألة ويوفر الاشراف على ضمان التخفيف من المخاطر بشكل مناسب بينما تضمن الادارة تنفيذ الضوابط للتخفيف من المخاطر.

يعتبر معيار (ISO/IEC 27001:2013) المعيار الدولي الذي يبين كيفية وضع نظام إدارة المخاطر السيبرانية وتطبيقه والحفاظ عليه وتحسينه باستمرار، ضمن أطر عملية مما يسمح بالحفاظ على البيانات الحساسة والسرية بشكل آمن والتقليل من احتمال الوصول إليها بشكلٍ غير قانوني أو بدون إذن كما يسمح بإدارة المخاطر السيبرانية واسترداد المعلومات وتقليل الخروقات الأمنية وتم نشر المعيار للمرة الاولى عام 2005 وتم اجراء العديد من التعديلات عليه اخرها سيتم الاعلان عنه في تشرين الثاني 2022.

٢-الثغرات: ضعف في النظم السيبرانية والتي تسمح للمهاجم الالكتروني اختراقها نتيجة عدم اكتشافها من قبل الجهة المالكة.

٣-المخاطر السيبرانية: الهجمات والتهديدات من قبل المخترقون مما ينعكس على امن الحوسبة السحابية للمالك.

يتكون المؤشر المقترح من الابعاد الخمس الآتية- :

١- حوكمة الامن السيبراني ويتضمن (١٠) مؤشرات وكالآتي- :

١-الاستراتيجيات المتبعة للأمن السيبراني

٢-إدارة الامن السيبراني من قبل مجلس إدارة الشركة

٣-لجان الامن السيبراني محددة بموجب أوامر إدارية وصلاحيات محددة

٤-إدارة مخاطر الامن السيبراني

٥-جودة برامج صد الهجمات السيبرانية وحماية الفضاء السيبراني تخضع للتدقيق من قبل قسم التدقيق السيبراني.

٦-الامن السيبراني للأفراد العاملين الداخليين

٧-الامن السيبراني للزبائن المتعاملين مع الوحدة الاقتصادية

٨-المراجعة المستمرة لجودة الخطط الاستراتيجية للحد من مخاطر الامن السيبراني من قبل مجلس الإدارة

٩-وضع دليل استرشادي لمخاطر الامن السيبراني

١٠-الالتزام بالتشريعات والقوانين واللوائح الصادرة عن البنك المركزي العراقي او الجهات الحكومية التشريعية بخصوص الامن السيبراني.

ب: حماية الامن السيبراني ويتضمن (6) مؤشرات وكالآتي- :

١-إدارة الأصول السيبرانية

٢-إدارة صلاحيات استعمال الأجهزة الالكترونية

٣-إدارة امن الفضاء السيبراني

٤-حماية البريد الالكتروني ووسائل التواصل الرقمي الذي تعتمده الشركة والموقع الالكتروني الرسمي

٥-إدارة النسخ الاحتياطية

٦-اختبارات الاختراق والتشفير والحماية للسجلات الرقمية

ج: الاستراتيجية (الرؤية المستقبلية) ويتضمن (5) مؤشرات وكالآتي- :

١-الموقع الالكتروني للوحدة الاقتصادية

٢ -الإدارة الأمنية السيبرانية وفق التشريعات والتعليمات والاستراتيجية المعتمدة في البلد المعني.

٣-استراتيجيات التحسن المستمر والإجراءات الكفيلة بتوصيل المعلومات لمتخذي القرارات

٤-لجنة استراتيجية لإدارة المخاطر السيبرانية

٥-الإفصاح عن الأسلوب وإجراءات الامن السيبراني في الوحدة الاقتصادية

د: إدارة المخاطر السيبرانية ويتضمن (4) مؤشرات وكالآتي- :

١-وصف الامن السيبراني ومخاطر المعلومات المتاحة والتي تعرض لها الوحدة الاقتصادية والحالات التي تمكنت بها الوحدة في صد الهجوم السيبراني.

٢-عدد التقارير المرفوعة الى الإدارة العليا من قبل لجنة إدارة المخاطر عن حالات الاختراق.

٣-توظيف مستشار باختصاص برمجيات الحاسوب

٤-عدد الحالات التي أسهم بها التدقيق الداخلي في إدارة مخاطر الانترنيت

هـ - الاثار المالية ويتضمن (8) مؤشرات وكالآتي- :

1-التكاليف المدفوعة لتعزيز الامن السيبراني في الوحدة الاقتصادية

2 -التامين المدفوع لشركات التامين للحفاظ على خصوصية الجهات الخارجية المتعاملة مع الوحدة ضداي هجوم سيبراني

3 -الافصاح عن الخسائر المالية التي تترتب عن انتهاكات الفضاء السيبراني للشركة

4-الدعم المالي لتطوير البرامج الالكترونية لحماية وتعزيز الامن السيبراني

5 -الدعم المالي المقدم لإجراءات تقييم وتحسين اجراءات المخاطر السيبرانية القبلية والبعدية

6 -الافصاح عن الدورات التدريبية (مبالغها) المنعقدة داخل وخارج العراق

7-الافصاح عن السجلات الخاصة بالموجودات المعلوماتية والتقنية وترميزها وفقا للمتطلبات التشريعية والمعاهدات المحلية والدولية

8- المبالغ المتكبدة للتعافي من الهجمات السيبرانية السابقة والاجراءات البديلة لضمان استمرار العمل في حالة حصول هجوم سيبراني

2.4 اختبار المؤشر المقترح على (عينة) من المصارف:

لغرض اختبار المؤشر المقترح على المصارف العراقية المدرجة في سوق العراق للأوراق المالية وعلى وفق مجتمع البحث المتكون من 38 مصرفا مدرج في السوق الانف الذكر فان عينة البحث تم اختيارها على وفق تعاملاتها وانشطتها التي تعتمدها على المعاملات الرقمية وتم اختيار عينة من هذه المصارف تمثلت بأربع مصارف (مصرف بغداد التجاري، مصرف الخليج التجاري ، المصرف العراقي التجاري ومصرف الاهلي التجاري) ،وتم اختيار السنوات (2019-2020) بحكم ازدياد التعاملات السيبرانية في ظل جائحة كوفيد -19 ولقياس مستوى الافصاح عن المخاطر السيبرانية على وفق المؤشر المقترح سيتم الاعتماد على المعادلة التالية:

مستوى الافصاح وفق المؤشر المقترح = (المتطلبات المفصح عنها /اجمالي مؤشرات المقياس الفرعية)*100، وبوضح الجدول (4) نسب الافصاح لعينة البحث عن متطلبات الافصاح عن مخاطر الامن السيبرانية

الجدول 4: نسب الافصاح لعينة البحث عن متطلبات الافصاح عن مخاطر الامن السيبرانية

	التفاصيل	السنوات/المصارف							
		9201				2020			
البعد الرئيس للمؤشر	المؤشرات	B*	K*	I*	*A	B	K	I	A
حوكمة الامن السيبراني	1-وصف الامن السيبراني ومخاطر المعلومات المتاحة والتي تعرض لها الوحدة الاقتصادية والحالات التي تمكنت بها الوحدة في صد الهجوم السيبراني.	1	0	0	0	1	0	0	0

	٢-عدد التقارير المرفوعة الى الإدارة العليا من قبل لجنة إدارة المخاطر عن حالات الاختراق.	0	0	1	1	0	0	0	1
	٣-توظيف مستشار باختصاص برمجيات الحاسوب	1	1	1	1	1	1	1	1
	٤-عدد الحالات التي أسهم بها التدقيق الداخلي في إدارة مخاطر الانترنيت	0	0	0	0	0	0	0	0
حماية الامن السيبراني	المجموع	2	1	1	3	1	1	1	2
	١-إدارة الأصول السيبرانية	0	1				1	1	1
	٢-إدارة صلاحيات استعمال الأجهزة الالكترونية	1	1	1	1	1	1	1	1
	٣-إدارة امن الفضاء السيبراني	1	0	1	1	0	1	1	1
	٤-حماية البريد الالكتروني ووسائل التواصل الرقمي الذي تعتمده الشركة والموقع الالكتروني الرسمي	1	0	0	0	0	0	0	0
	٥-إدارة النسخ الاحتياطية	1	1	1	1	1	1	1	1
	٦-اختيارات الاختراق والتشفير والحماية للسجلات الرقمية	0	0	0	0	0	0	0	0
	المجموع	4	3	3	4	2	3	4	4
الاستراتيجية	١-الموقع الالكتروني للوحدة الاقتصادية	1	1	1	1	1	1	1	1
	٢- الإدارة الأمنية السيبرانية وفق التشريعات والتعليمات والاستراتيجية المعتمدة في البلد المعني.	0	1	1	1	1	1	1	1
	٣-استراتيجيات التحسن المستمر والإجراءات الكفيلة بتوصيل المعلومات لمتخذي القرارات		0	0	0	0	0	0	0
	٤-لجنة استراتيجية لإدارة المخاطر السيبرانية	0	0	0	0	0	0	0	0

	٥-الإفصاح عن الأسلوب وإجراءات الامن السيبراني في الوحدة الاقتصادية	0	0	0	0	0	0	0
	المجموع	1	2	2	2	2	2	2
ادارة المخاطر السيبرانية	١-وصف الامن السيبراني ومخاطر المعلومات المتاحة والتي تعرض لها الوحدة الاقتصادية والحالات التي تمكنت بها الوحدة في صد الهجوم السيبراني.	0	0	0	0	0	0	0
	٢-عدد التقارير المرفوعة الى الإدارة العليا من قبل لجنة إدارة المخاطر عن حالات الاختراق.	0	0	0	0	0	0	0
	٣-توظيف مستشار باختصاص برمجيات الحاسوب	1	1	1	1	1	1	1
	٤-عدد الحالات التي أسهم بها التدقيق الداخلي في إدارة مخاطر الانترنيت	0	0	0	0	0	0	0
	المجموع	1	1	1	1	1	1	1
الاثار المالية	١-التكاليف المدفوعة لتعزيز الامن السبراني في الوحدة الاقتصادية	0	0	0	0	0	0	0
	٢- التامين المدفوع لشركات التامين للحفاظ على خصوصية الجهات الخارجية المتعاملة مع الوحدة ضداي هجوم سيبراني	0	0	0	0	0	0	0
	٣- الافصاح عن الخسائر المالية التي تترتب عن انتهاكات الفضاء السيبراني للشركة	0	0	0	0	0	0	0
	٤-الدعم المالي لتطوير البرامج الالكترونية لحماية وتعزيز الامن السيبراني	1	0	0	1	1	1	1
	٥- الدعم المالي المقدم لاجراءات تقييم وتحسين اجراءات المخاطرالسبرانية القبلية والبعدية							

	٦- الافصاح عن الدورات التدريبية (مبالغها) المنعقدة داخل وخارج العراق	1	1	1		1	1	1	1
	٧-الافصاح عن السجلات الخاصة بالموجودات المعلوماتية والتقنية وترميزها وفقا للمتطلبات للمتطلبات التشريعية والمعاهدات المحلية والدولية.	0	0	0	0	0	0	0	0
	المجموع	2	1	1	1	1	2	2	2

المصدر: اعداد الباحثون *

للدلالة على مصرف بغداد التجاريB

مصرف الخليج التجاريK*

المصرف العراقي التجاري*I

مصرف الاهلي التجاري*A

من الجدول (4) يتضح ان هناك تباين في الافصاح عن مخاطر الامن السيبراني في المصارف عينة البحث على وفق المؤشر المقترح من الباحثين ويوضح الجدول (5) متوسط نسب الافصاح عن الابعاد الرئيسة للمؤشر المقترح في عينة البحث.

الجدول 5: متوسط نسب الافصاح عن الابعاد الرئيسة للمؤشر المقترح واختباره في عينة البحث

الفقرات	مصرف بغداد التجاري		مصرف الخليج التجاري		العراقي التجاري		المصرف الاهلي التجاري	
	2019	2020	2019	2020	2019	2020	2019	2020
حوكمة الامن السيبراني	50	75	25	25	25	25	25	50
حماية الامن السيبراني	66	66	50		50	66	33	66
الاستراتيجية	40	40	40	60	40	60	40	40

ادارة المخاطر السيبرانية	25	25	25	25	25	25	25	25
الاثار المالية	20	20	20	20	20	0	20	0

المصدر – اعداد الباحثون

من الجدول (٤) يتضح ان هناك تفاوت في افصاح المصارف عينة البحث عن المخاطر السيبرانية الا ان الملاحظ ان الاهتمام اخذ بالتزايد مقارنة بين (٢٠١٩-٢٠٢٠) حيث ظهرت النسب اعلى في العام ٢٠١٩ وذلك بحكم التغيرات التي طرأت على البيئة المصرفية واثار جائحة كوفيد-19 والتحول من العمل اليدوي الى العمل الالكتروني وازدياد المخاطر السيبرانية المرافقة لهذا العمل وبالتالي:

١-حوكمة الامن السيبراني: بلغ متوسط الإفصاح عن حوكمة الامن السيبراني على وفق المؤشر المقدم والمتكون من أربع مقرات بنسب متفاوتة، حيث بلغ الإفصاح في المصارف عينة البحث لعام ٢٠١٩(٥٠٪،٢٥٪،٢٥٪،٢٥٪) على التوالي في المصارف عينة البحث (بغداد التجاري، مصرف الخليج التجاري، مصرف العراق التجاري، مصرف الأهلي التجاري)في حين بلغت نسب الإفصاح عن البعد حوكمة الامن السيبراني لعام ٢٠٢٠ (٧٥٪، ٢٥٪، ٢٥٪، ٥٠٪) حيث يبرز مصرف بغداد التجاري كأحد المصارف المهمة بالإبلاغ والاهتمام بحوكمة الامن السيبراني يليه مصرف الأهلي التجاري وبنفس النسب المصرف الخليج التجاري والمصرف العراق التجاري.

٢-حماية الامن السيبراني: بلغ متوسط الإفصاح عن حماية الامن السيبراني على وفق مؤشر المقترح والمتكون من (٦) مقرات بنسب متفاوتة لعام ٢٠١٩ حيث بلغت (٦٦٪، ٥٠٪، ٥٠٪، ٣٣٪) لمصارف (بغداد التجاري، مصرف الخليج التجاري، مصرف العراق التجاري، مصرف الأهلي التجاري) على التوالي وهي نسبة جيدة نسبيا وفي عام ٢٠٢٠ حافظت المصارف على نفس نسبة الإفصاح تقريبا (٦٦٪) بخلاف مصرف الأهلي التجاري التي ارتفعت نسبة الإفصاح لدرجة تصل الى (٦٦٪).

٣-الاستراتيجية: بلغ متوسط الإفصاح عن الاستراتيجية والمتكون من خمس مقرات بنسب متفاوتة للمصارف عينة البحث لعام ٢٠١٩ وكالتالي: (٢٠٪، ٤٠٪، ٤٠٪، ٤٠٪) في حين حققت المصارف نسب متقاربة (20٪، ٤٠٪، ٤٠٪، ٤٠٪) للمصارف (بغداد التجاري والخليج التجاري والمصرف العراقي التجاري والمصرف الأهلي التجاري) على التوالي.

4 –ادارة المخاطر السيبرانية: وبعدد فقرات المؤشر (5) حققت المصارف عينة البحث النسب المتساوية لعامي (2019 –2020) (25%)، مما يدل على ان الاهتمام متساوي للسنتين وبنسبة ضعيفة رغم ازدياد المخاطر السيبرانية لسنة 2020

5 –الاثار المالية: وب٧فقرات حققت المصارف نسب متفاوتة في الإبلاغ عن متطلبات المؤشر المقترح حيث حققت المصارف عينة البحث لعام ٢٠١٩ على التوالي (٢٨٪، ١٤٪، ٢٨٪، ٢٨٪) وفي عام ٢٠٢٠(١٤٪، ١٤٪، ٢٨٪، ٢٨٪). للمصارف (بغداد التجاري، مصرف الخليج التجاري، مصرف العراقي التجاري، مصرف الأهلي التجاري).

تأسيسا لما تقدم فأن هناك تباين في الإفصاح عن الابعاد الحتمية وعلى وفق المؤشر المقترح للإفصاح عن مخاطر السيبرانية وهذا يدل على ان هناك اهتمام بالإفصاح عن المخاطر السيبرانية في عينة المصارف المدرجة في سوق العراق للأوراق المالية وعلى وفق ذلك يتم قبول فرضية البحث.

5. خاتمة:

خرج البحث بالعديد من الاستنتاجات والتوصيات نورد أبرزها :

أولا: الاستنتاجات:

١–برز الاهتمام وبشكل كبير جدا بالإفصاح عن المخاطر السيبرانية خصوصا بعد ازدياد الهجمات السيبرانية على جميع القطاعات خصوصا قطاع المصارف بعد ازدياد أنشطتها التي تعتمد على الحوسبة السحابية.

٢–المحاسبة متكيفة ومتواصلة مع التغيرات التي تطرأ على البيئة لذا سعت الهيئات المهنية الى تأطير عملية الإفصاح عن المخاطر السيبرانية من خلال الأدلة والارشادات ومن هذه الجهات SEC, AICPAومعايير .SAB

٣–المؤشر المقترح للإفصاح عن مخاطر الامن السيبراني في البيئة العراقية يتوافق مع طروحات الهيئات المهنية الدولية مع استراتيجية الامن السيبراني في البيئة العراقية.

٤–على الرغم من غياب التعليمات المنظمة للإفصاح عن المخاطر السيبرانية في البيئة العراقية في سوق العراق للأوراق المالية الا ان المصارف عينة البحث كانت تفصح عن المخاطر السيبرانية وبنسب متفاوتة.

ثانيا: التوصيات:

١-تضمين مخاطر الامن السيبراني كأحد المقررات الدراسية في مرحلة البكالوريوس لأقسام المحاسبة والمالية والمصرفية وتشجيع طلبة الدراسات العليا على الخوض بهكذا مجال بحثي.
٢-تبني المؤشر المقترح للإفصاح عن مخاطر الامن السيبراني في سوق العراق للأوراق المالية والعمل على ان تصدر هيأة الأوراق المالية التعليمات المنظمة للإفصاح عن المخاطر في السوق.
٣-عمل الجهات الرقابية في البيئة العراقية على التعاون مع هياة سوق العراق للأوراق المالية لتوفير المتطلبات الأساس لتدقيق الإفصاح عن تقارير المخاطر السيبرانية.

6. قائمة المراجع:

أولا: العربية

النشرات والقوانين والتعليمات والأدلة الاسترشادية

١-قانون سوق العراق للأوراق المالية رقم (٧٤) لسنة (٢٠٠٤) المعدل
٢-تعليمات الإفصاح في سوق العراق للأوراق المالية رقم (١٨) لسنة (٢٠١٥) المعدل
٣-نشرة الاتحاد المصري للتأمين ٢٠١٩، عدد خاص لهجمات السيبرانية صادرة عن الاتحاد العربي للتأمين العدد رقم (٦٧)
٤-الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١) المجلس الأعلى للأمن السيبراني رئاسة مجلس الوزراء، جمهورية مصر العربية /ص(١-١٩)
٥-الدليل التنظيمي للأمن السيبراني،٢٠٢٠، هيئة الاتصالات وتقنية المعلومات، السعودية/ص (١-٥٤)
٦-تعليمات التكيف مع المخاطر السيبرانية ،٢٠١٨، البنك المركزي الأردني، ص (١-٣٢)
٧-الهيئة الوطنية للأمن السيبراني،٢٠١٨، السعودية، ص (١-٤٠)
٨-استراتيجية الامن السيبراني العراقي ٢٠١٩، مستشارية الامن الوطني امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات ص (١-١٥)
٩-الامن السيبراني في العراق: قراءة في مؤشر الامن السيبراني العالمي، ٢٠٢٠، نشرات مركز البيان للدراسات والتخطيط، العراق

الدوريات والمؤتمرات:

١-الرشيدي، طارق عبد العظيم والسيد عباس ،٢٠١٩، (إثر الإفصاح عن مخاطر الامن السيبراني في التقارير المالية على مصادر الأسهم واحجام التداول: دراسة مقارنة في قطاع التكنولوجيا المعلومات)، مجلة المحاسبة والمراجعة، العدد الثاني ص (٤٣٩-٤٨٧)

٢-علي، محمود احمد وعلي صالح، ٢٠٢٢(إثر الإفصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة (تحديات وافاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين) للفترة من (١٠-١١، ٢٠٢٢(

٣-صالح، نرمين محمد (محددات فعالية المراجعة الداخلية للأمن السيبراني)، ٢٠٢٢، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة (تحديات وافاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين) للفترة من (١٠-١١، ٢٠٢٢)

ثانياً: الأجنبية:

1-Eaton, T., V., Grenier, J. HS Layman, D., (2019), »Accounting and cybersecurity risk management », current issue in Auditing, 13(2), c1-c9.

2-Li, Nean, G., I. And Wang. T.,(2018), « SEC'S cybersecurity disclosure, guidance and disclosure cybersecurity risk factors », international journal of accounting information system(pp.40-55).

3-Yang, L., Lau, L. and Jan, H.,(2020) investors' perceptions of the cybersecurity risk management reporting framework, international journal of accounting and information management, vol.28, pp.167-183.

4-kelton, A., pennington, R., (2020), (Dovdonatory disclosures miligate the cybersecurity breach contagion effect? journal of information system, 34(3): pp:133-150.

5-AICPA unveils cybersecurity risk management reporting framework, (2017), New York, April, 2017.CPA, CGMA.

6-Fortin, Anne and Heroux, S., (2020), (Cybersecurity disclosure by the companies on the SPP/TSX60, index, vol:19, issue:2, June, pp:73-100.

7-Ramirez, M, Ariza, L., and Miranda, M, (2022), (The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index), journal of sustainability ,2022,14(3).