# مؤشر مقترح للإفصاح عن المخاطر السيبرانية في سياق بيئة المعلوماتية المصرية الرقمية

إعداد

د / عمرو عادل عبدالفتاح موسى

قسم المحاسبة والمراجعة

كلية التجارة – جامعة مدينة السادات

٢٠٢٥م – ١٤٤٦هـ

قسم المحاسبة والمراجعة ... كلية التجارة ... جامعة مدينة السادات

## مقدمة :

بلغت قيمة سوق الأمن السيبراني ١٥٠.٣٧ مليار دولار في عام ٢٠٢١، ومن المتوقع أن تصل قيمته إلى ٣١٧.٠٢ مليار دولار بحلول عام ٢٠٢٧ (Mordor Intelligence, 2022, p1; Sonic Wall, 2022; p5). كما تقدر التكلفة العالمية للجرائم السيبرانية بـ٦ تريليون دولار سنوياً ومن المتوقع أن تنمو إلى ١٠.٥ تريليون دولار في عام ٢٠٢٥، ولهذا السبب لا توجد طريقة للبقاء في مأمن، إلا في وجود ضوابط داخلية جيدة (O'Connell, 2023, p3). ومع تزايد التحول الرقمي والرقمنة السريعة، يتزايد التهديد السيبراني ضد منشآت الأعمال بوجه عام، والمنشآت المالية بوجه خاص (Gulyas & Kiss, 2023, p85).

وتؤثر هذه المخاطر السيبرانية في المقام الأول على القطاعات التكنولوجية والمالية بأسوأ طريقة ممكنة (Lenka et al., 2023, p172). ولا تزال المنشآت التي تجمع البيانات وتخزنها وتستخدمها، تتحمل مخاطر مالية غير معروفة من انتهاك محتمل للبيانات (Theriot & Gowan, 2023, p2). والقطاع المصرفي هو أحد القطاعات التي تتأثر بشكل جوهري بالمخاطر السيبرانية (Rahmawati, 2024, p2). وهو ما أشارت إليه دراسة (Wang et al., (2024, p16، والتي أكدت على أن قطاع الخدمات المالية وقطاع الاتصالات والمعلومات، والقطاعات ذات الكثافة التكنولوجية العالية، هي من أكثر القطاعات تعرضاً للمخاطر السيبرانية.

ولتحسين التواصل مع المستثمرين، تحتاج المنشآت إلى تقديم إفصاحات تتعلق بالأمن السيبراني ومخاطره، والإستجابة لها والتخفيف من حدتها في تقاريرها السنوية (Ibrahim et al., 2021, p12; Cao et al., 2023, p6081). فضلاً عن كيفية معالجة هذه المخاطر، وليس لديهم عموماً خيار سوى الاعتماد على إفصاحات الشركات عن المخاطر السيبرانية، بسبب عدم تماثل المعلومات بين المنشآت وبعضها البعض (Cheong et al., 2021, p180). وتؤثر المخاطرالسيبرانية بسبب الإهمال والتعامل غير الصحيح مع البيانات المحاسبية الحساسة للغاية على موثوقية التقارير المالية (Elnagar et al., 2024, p2505).

كما أكدت دراسة Jiang et al., (2022) على أن الإفصاح عن طبيعة المخاطر السيبرانية وإدارتها، هي إحدى الطرق التي يمكن من خلالها التواصل مع أصحاب المصالح، وينبغي أن تنعكس المخاطر السيبرانية المؤكدة والمحتملة على توفير إفصاحات إضافية للمنشأة في القوائم والتقارير السنوية. وعندما تفصح منشأة ما عن معلومات الأمن السيبراني في تقريرها السنوي، فإن ذلك يعطي إشارة السوق مفادها أن المنشأة تشارك بنشاط في منع الاختراقات الأمنية واكتشافها وتصحيحها (Lenka et al., 2023, p175).

وفي هذا السياق، يمكن أن تؤثر المخاطر السيبرانية بشكل جوهري على العمليات التجارية وسلامة التقارير المالية (Ramírez et al., 2022, p8). كما أن هناك حاجة إلى تقارير مالية موثوقة مدفوعة بالحاجة إلى ضوابط الأمن السيبراني حول أنظمة المحاسبة المالية

للمنشأة (Pfanstiel, 2022, p10). ويتوقع المستثمرون رؤية المزيد من المعلومات المتعلقة بالمخاطر السيبرانية، خاصةً إذا لم تفصح المنشأة عن أي معلومات حول هذه المخاطر سابقاً (Remeis, 2023, p11). وعندما يكون للأمن السيبراني القدرة على التأثير على البيانات المالية بشكل جوهري، فإنه يصبح قضية محاسبية، ويتطلب دمجه في النظام المحاسبي (Wang, 2024, p2).

وصرح المعهد الأمريكي للمحاسبين القانونيين (AICPA, 2018, p1) بأنّ الأمن السيبراني هو أحد أهم القضايا التي تشغل بال مجالس الإدارة في كل منشأة. ووضع إطار عمل للتقرير عن هذه المخاطر، من خلال ثلاث أجزاء رئيسية من المعلومات وهي: وصف الإدارة لبرنامج إدارة المخاطر السيبرانية للمنشأة، وتأكيدات الإدارة بشأن فعالية ضوابط الأمن السيبراني، ورأي المراجع بشأن إفصاحات الإدارة (الرشيدي، عباس، ٢٠١٩، ص ٤٤٥؛ Kelton & Pennington, 2021, p.137). وتتبنى حوالي ٢٩% من المنشآت في (S & P 500) اختيارياً هذا الإطار(Frank et al., 2023, p2). ولجعل المنشآت مسؤولة وأكثر شفافيةً بشأن مخاطرها السيبرانية وإدارتها، أصدرت الهيئات التنظيمية مبادئ وإرشادات توجيهية بشأن الافصاح عن الأمن السيبراني ومخاطره ( Firoozi & Mohsni, 2023, p1).

كما ركزت الجهات التنظيمية اهتمامها على كيفية معالجة ومراقبة المخاطر السيبرانية في التقارير المالية (Bricker et al., 2022; Hughes et al., 2023, p4). ولذلك حثت الجهات التنظيمية المنشآت على تعزيز المعلومات الخاصة بالإفصاح عن المخاطر السيبرانية في التقارير المالية ( Bansal & Axelton, 2023, p1; Gordon et al., 2024, p2). وذلك لمحاولة التخفيف من أي مخاطر محتملة أو حدثت بالفعل، وذلك من خلال زيادة الشفافية التي ستبني ثقة جميع أصحاب المصلحة Lenka et al., 2023, (p169). وأن الشركات والمستثمرين سيستفيدون إذا كانت هذه المعلومات مقدمة بطريقة متسقة وقابلة للمقارنة ومفيدة لاتخاذ القرارات (Jiang et al., 2024, p146).

وفي الواقع، أدت الحاجة إلى إدارة سرية المعلومات ونزاهتها وتوافرها، إلى قيام مجالس إدارة المنشآت بالنظر في المخاطر السيبرانية، وبالتالي أصبح الأمن السيبراني مؤخراً جزءاً من الفهم السائد ومجال التحقيق من قبل حوكمة الشركات، وستستجيب معايير المحاسبة المستقبلية لضرورة الإفصاح عنها مع ضرورة حماية البيانات الحساسة ( Napolitano, 2023, p2). وبذلك حظي الإفصاح عن المخاطر السيبرانية باهتمام كبير من جانب أصحاب المصالح، كاستجابة لطلبهم للحصول على مزيد من المعلومات حول هذه المخاطر (شرف، ٢٠٢٣، ص٢١٤). ولذلك فإن المنشآت بحاجة إلى الإفصاح عن المخاطر السيبرانية التي تواجهها أو التي يتوقع أن تواجهها مستقبلاً، وذلك لتعزيزالإفصاح والشفافية في تقاريرها السنوية (مسعود & عبدالفتاح، ٢٠٢٤، ص ١١؛ Tadesse et al., 2024, p5).

واتجهت التحديثات الأخيرة نحو الإفصاح عن المخاطر السيبرانية، سواء كانت كمية أو نوعية، في تقارير البنوك والشركات (Shehata et al., 2023, p4, 5). ووفقاً لنظرية أصحاب المصلحة، فإن الحوكمة الجيدة للشركات تضمن المصالح طويلة الأجل لجميع الأطراف، وخاصةً في إدارة المخاطر السيبرانية، ويمكن أن يؤدي الإفصاح الفعال عن المخاطر السيبرانية إلى تقليل عدم تماثل معلومات بشكل جوهري، مما يزيد بوضوح فعالية استراتيجيات وتدابير الأمن الخاصة بالمنشأة، وبالتالي تضييق فجوة الثقة بين المنشأة والعالم الخارجي (Guohong et al., 2025, p5). حيث ينبغي على المنشآت النظر في تطبيق أطر عمل موحدة للإفصاح عن المخاطر السيبرانية، تتضمن مقاييس محددة لتقييم التعرض للمخاطر وفعالية استراتيجيات التخفيف منها (Abdelraouf& Hussainey, p1).

وفي ضوء ماسبق، تسعي هذه الورقة إلى تسليط الضوء على آليات الإفصاح عن المخاطر السيبرانية، وإستخلاص مؤشر محاسبي مقترح لآليات الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها، وذلك بالإرتكاز على التوجيهات والإرشادات المحاسبية الصادرة من قبل الجهات المهنية والتنظيمية، ودراسة وتحليل الآثار الجوهرية لهذه الإفصاحات على القوائم المالية والتقارير السنوية والإفصاحات ذات الصلة، وبما يتلائم مع بيئة الأعمال المصرية في ضوء التحول الرقمي والحوكمة السيبرانية والرقمنة.

وتأسيساً على ماسبق، تركز هذه الورقة على التعمق في مجال الإفصاح عن المخاطر السيبرانية، وحوكمة إدارتها، وكيفية الافصاح عن سيناريوهات معالجتها والتخفيف من حدتها، وإستجابة للدعوات البحثية في عدد من الدراسات السابقة، والتي كانت بمثابة تساؤلات ومناقشات علمية لدراسات مستقبلية حول هذه المتغيرات، وفي ظل إهتمام الدول بالأمن السيبراني مع تشكيل هيئات ومجالس عليا بإصدار العديد من الضوابط والإرشادات والمبادرات المتعلقة بالمخاطر السيبرانية، وخاصةً في ظل توجه الدولة المصرية نحو الشمول المالي والرقمنة، ومحاولة التغلب على أوجه القصور في مثل هذه الدراسات لاسيما في بيئتنا العربية.

**وتبرز أهمية هذه الورقة البحثية من خلال عدة نواحٍ، فنظرياً تحاول تسليط الضوء على طبيعة المخاطر والتهديدات السيبرانية التي تتعرض لها منشآت الأعمال، وآليات الإفصاح عن المخاطر السيبرانية وحوكمة إدارتها ومعالجتها والمحددات والصعوبات التي تواجه تطبيق هذه الإفصاحات، وتطبيقياً، إرساء الضوابط والأطر المنهجية بشان الافصاح عن الأمن السيبراني ومخاطره، وتحديد الأولويات وتنظيم المعلومات حول المخاطر الفعلية والمحتملة التي تهم جميع الأطراف، لتوفير المعلومات الملائمة.**

**وستركز هذه الورقة على تقديم مؤشر مقترح للإفصاح عن المخاطر السيبرانية يلائم طبيعة الأعمال المصرية في عصر الرقمنة، دون التطرق إلى الجوانب التقنية والبرمجية لتأمين البيانات، والحد من هجمات المخاطر السيبرانية**. ولتحقيق الهدف من تلك الورقة سيتم تقسيم ما تبقى بناءً على المحاور التالية :

- **المحور الأول: ماهية وأنواع المخاطر السيبرانية.**
- **المحور الثاني: ماهية ومتطلبات الافصاح المحاسبي عن المخاطر السيبرانية.**
- **المحور الثالث: مؤشر الإفصاح المقترح عن المخاطر السيبرانية وحوكمة إدارتها.**
- **المحور الرابع: خلاصة الورقة ومجالات البحث المستقبلية.**

## المحور الأول: ماهية وأنواع المخاطر السيبرانية.

### ١- طبيعة المخاطر السيبرانية:

تعددت وجهات نظر الباحثين والجهات التنظيمية، فيما يتعلق بمفهوم المخاطر السيبرانية. فقد عرفتها الهيئة المصرية للأمن السيبراني المصري، (٢٠١٨، ص١١٩) بأنها المخاطر التي يمكن أن تواجه المنشآت بما فيها رسالة المنشأة ورؤيتها أوسمعتها، بسبب إمكانية الوصول غير المصرح أوسوء الاستخدام أوتدمير المعلومات. ووصفتها دراسة (Varga et al., 2021, p9) بأنها مخاطر تشغيلية غير مالية بغض النظر عن المنشأ، وهذه المخاطر تنطوي على تكاليف.

في حين عرفتها عرفتها دراسة كل من (Strupczewski , (2021, p6); Smaga, 2024, p3) بأنها مخاطر تشغيلية مرتبطة بأداء الأنشطة في الفضاء السيبراني، مما يهدد أصول المعلومات، وموارد تكنولوجيا المعلومات والاتصالات والأصول التكنولوجية، التي قد تسبب أضراراً مادية للأصول الملموسة وغير الملموسة للمنشأة. وتشمل التهديدات المادية لإعادة مصادر تكنولوجيا المعلومات والاتصالات داخل المنشأة Heidenborg & (Lappalainen, 2021, p2).

وتنطوي المخاطر السيبرانية على حدث سيبراني ضار يسبب تعطل الأعمال التجارية والخسارة النقدية (Pacheco-Paredes & Wheatley, 2022, p2, 6). وتعرف بأنها حدوث خسائر محتملة تتحقق عندما يؤثر التهديد السيبراني على أحد الأصول ذات القيمة ويؤدي إلى تأثير جوهري على المنشأة (CLInton & PeIFeR, 2022, p14). وعرفتها دراسة Pfanstiel, (2022, p10) بأنها الآثار التي تم تحديدها لحادث أمن بيانات كبير محسوباً على أساس الخسائر المالية بما في ذلك التكاليف الخاصة والتكاليف الخارجية، وتكلفة العوامل الخارجية هي التكاليف غير المباشرة المتكبدة بسبب انتهاكات الأمن السيبراني التي تحدث لمنشآت أخرى داخل الصناعة.

ولقد عرف مجلس الاستقرار المالي المخاطر السيبرانية، لأغراض إدارة المخاطر المالية، على أنها "مزيج من احتمال وقوع الحوادث السيبرانية وتأثيرها". (Ferens, 2021, p36; Jin et al., 2023, p1; Bek-Gaik & Surowiec, 2024, p1516). وقد أكدت دراسة كل من (Hartmann & Carmenate, (2021); Florackis et al., (2023, p352 على أنها مخاطر الخسارة المالية أوالانقطاع التشغيلي أوالإضرار بسمعة المنشأة، نتيجة الفشل في أنظمة تكنولوجيا المعلومات الرقمية. ويمكن النظر إلى المخاطر السيبرانية باعتبارها خطراً ناتجاً عن عدم الامتثال للمسؤولية الاجتماعية للشركات (Khan et al., 2025, p1).

**وفي ضوء ما سبق، يري الباحث أنها عبارة عن مدى تعرض أنظمة الوحدة الاقتصادية لخسائر (مالية وغير مالية) واسعة النطاق، وغير متوقعة ونتائج غير مرغوب فيها، نتيجة حدوث تهديدات محتملة غير مؤكدة للإضرار بسرية ونزاهة وتوافر البيانات والمعلومات الخاصة بالمنشأة في الفضاء السيبراني، مما يؤثر على قدرتها على تحقيق أهدافها واستمراريتها في حالة وقوع هذه المخاطر.**

## ٢- أنواع (تصنيفات) المخاطر السيبرانية التي تهدد حماية المعلومات المحاسبية:

باستقراء الفكر المحاسبي فيما يتعلق بتصنيف المخاطر السيبرانية التي تواجهها المنشآت، لا تتعرض كل الصناعات بشكل متطابق للمخاطر السيبرانية. ويتوقف ذلك على عدة عوامل مثل طبيعة المخاطر وإمكانية حدوث خسائر، حيث تباينت الآراء حول التصنيفات المختلفة للمخاطر السيبرانية في القطاعات كالتالي: ( نشرة الاتحاد المصري للتأمين، ٢٠١٩، ص٣-١٧؛ يعقوب وآخرون، ٢٠٢٢؛ ص١٤١٤، جبر، ٢٠٢٢، ص ٩؛ مسعود& عبدالفتاح، ٢٠٢٤، ص ١٠؛ Wang et al., 2024,p 4):-

- **خطر سرقة أوفقدان البيانات،** البيانات الشخصية والبيانات التجارية، وأي بيانات ذات قيمة بالسوق تعتبر خطر، والدافع هوالبحث عن المكاسب المالية أوالتنافسية.
- **خطر تدمير البيانات،** مسح البيانات الإلكترونية أوتشفيرها أومنع الوصول إليها، والدافع هوالابتزاز.
- **خطر انقطاع الاتصالات،** تعطيل الموقع الالكتروني أوتعطيل الشبكة؛ تشويه الموقع للاستيلاء على صفحات وسائل التواصل الاجتماعي والدافع هوالابتزاز، والإرهاب، أوالتجسس.

كما اتفقت دراسة كل من شحاته والبردان، (٢٠٢١، ص١٠-١١)؛ السواح، (٢٠٢١، ص٥٠٦-٥١١)؛ Clemente, (2023, p22) على تصنيف المخاطر السيبرانية إلى ثلاث أنواع من المخاطر، وهي: (المخاطر المتعلقة بتأمين البيانات والمعلومات: وهي المخاطر الناشئة من تخرين البيانات والمعلومات للأفراد والمنشآت ومن الممكن تعرضها إلى الاختراق، أونقلها للمنافسين، والمخاطر المتعلقة بانتهاك الخصوصية: وهي المخاطر الناتجة عن مخاطر سرقة البيانات الشخصية، والمخاطر المتعلقة بانتهاك حقوق الملكية الفكرية: وتتمثل في المخاطر المتعلقة بحقوق الملكية الفكرية والأدبية نتيجة نسخ الوسائط الرقمية وإعادة إنتاجها).

ويصنف مجلس التقارير المالية (FRC) مخاطر الأمن الرقمي إلى (FRC, 2022, p3) : مخاطر الأمن الرقمي: هي المخاطر التشغيلية والمالية والمتعلقة بالسمعة وأصحاب المصلحة الناتجة عن تهديدات الأمن السيبراني، بما في ذلك مخاطر الانتهاكات الكبيرة للبيانات الناشئة عن الثغرات الداخلية، ومخاطر الاستراتيجية الرقمية: هي المخاطر التشغيلية والمالية والسمعة وأصحاب المصلحة الناتجة عن الانتقال إلى نموذج الأعمال الرقمية (يشار إليه أيضاً بالتحول الرقمي) وزيادة الاعتماد على البيانات.وأكدت دراسة كل من أميرهم،

(٢٠٢٢، ص ٣٣٩)؛ جبر، (٢٠٢٢)، ص٨؛ أبوالخير، (٢٠٢٣)، ص١٢؛ يوسف، (٢٠٢٤، ص ١٠)؛ Li et al., (2018, p45); Gulyás & Kiss, (2023, p86); Lestari et al., (2024, p17) على أن مخاطر الهجمات السيبرانية تضم ثلاث أنواع، كالتالي: -

أ- **مخاطر سيبرانية تتعلق بالسرية**: حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل المنشأة إلى أطراف ثالثة كما في حالة حدوث إختراق البيانات.وغالباً ستعاني المنشأة المخترقة من تكاليف السمعة.

ب- **مخاطر سيبرانية تتعلق باستمرارية الأداء (التوافر) :** والتي تتلخص في تعطل أوالتوقف عن ممارسة الأعمال، وتعرض توافر البيانات أوالنظم للخطر. ويمكن أن تتسبب أحداث التوافر في خسائر مباشرة وتكاليف تتعلق بالسمعة، بالإضافة إلى ذلك، يمكن أن تؤدي أحداث التوافر إلى شل حركة رأس المال والسيولة، وتؤثر على قدرة البنك على أداء أنشطته الأساسية، وبالتالي، يمكن أن يكون لمثل هذه الأحداث آثار غير مباشرة كبيرة على عملاء البنوك والمنشآت داخل وخارج القطاع المالي.

ت- **مخاطر سيبرانية تتعلق بالنزاهة:** والتي تتعلق بإساءة استخدام الأنظمة كما هوالحال بالنسبة للاحتيال، وتتعرض سلامة البيانات للخطر. ويمكن أن يكون لأحداث النزاهة تكاليف مباشرة مثل تكلفة استعادة سلامة البيانات والتكاليف القانونية لحل المشكلات التي لا يمكن فيها استعادة النزاهة، وعلى غرار أحداث التوافر، يمكن أن يكون لأحداث النزاهة تكاليف باهظة إذا أضعفت قدرة المنشأة على أداء أنشطتها الأساسية، وعلى وجه الخصوص، يمكن أن تؤدي أحداث النزاهة وما ينتج عنها من عدم تأكد قانوني إلى إطالة الوقت اللازم لاستعادة الأداء الكامل للمنشأة المتضررة والنظام على نطاق أوسع.

وقام الاتحاد الدولي للمحاسبين IFAC بتصنيفها إلي ثلاث أنواع هي: (مخاطر البنية التحتية لنظم تكنولوجيا المعلومات، ومخاطر تطبيق تكنولوجيا المعلومات، ومخاطر تكنولوجيا المعلومات الخاصة بأعمال المنشأة) (السواح، ٢٠٢١، ص٤٩٤؛ Heo, 2023, p5).

**ويري الباحث، أنه عند استخدام التصنيفات السابقة للمخاطر السيبرانية في تنظيم الأمن السيبراني المستمر للمنشأة، يتطلب كل نوع من أنواع المخاطر السيبرانية للبيانات المحاسبية طريقة محددة للوقاية والتجنب والقضاء على آثارها المحتملة، وهذا التصنيف المقترح سيحتاج إلى تعديل واستكمال بتغير التهديدات والمخاطر السيبرانية عبر الزمن.**

## المحور الثاني: ماهية ومتطلبات الافصاح المحاسبي عن المخاطر السيبرانية.

قد يؤدي الاعتراف بالمخاطر السيبرانية أن يدل على أن هناك مزيد من الجهود للحد من هذه المخاطر، ولكن عدم الافصاح عن تفاصيل ذلك في التقارير السنوية، قد يضلل أصحاب المصالح، ويقلل من قدرتهم على تقييم طريقة تعامل المنشأة معها ( Heidenborg & Lappalainen, 2021, p45). لذا ينبغي أن يتم إعلام المستثمرين بالمخاطر السيبرانية الجوهرية على المنشآت من خلال تقارير واضحة (أميرهم، ٢٠٢٢، ص ٣٤٦).

## ١ـ طبيعة وأهمية وخصائص الإفصاح المحاسبي عن المخاطر السيبرانية:

يعد الإفصاح عن المخاطر السيبرانية من المجالات البحثية التي نالت حيزاً واسعاً في المجال المحاسبي. حيث عرفته دراسة Kelton & Pennington, (2021, p139) بأنه الإفصاح عن المعلومات المتعلقة بحادث أمن البيانات، ويسمح بإيصال المعلومات إلى الأطراف المعنية فيما يتعلق بطبيعة وتأثير الخرق. ويقصد بنقص الإفصاح بأنه يتعلق بالنقص الذي يشمل أوجه القصور المحتملة (عدم وجود إفصاحات حول المخاطر السيبرانية، وعدم الإفصاح عن تأثير الخرق، وعدم الإفصاح عن استراتيجيات التخفيف من المخاطر السيبرانية) (Calderon & Gao, 2022, p3). ومن منظور سوق رأس المال، فإن التأثير المباشر للإفصاح عن المخاطر السيبرانية هوانخفاض عدم تماثل المعلومات بين المستثمرين حول الحوادث السيبرانية (Cao et al., 2024, p3). وعرفته دراسة ( Madani, (2024, p37، بأنه عملية توصيل المعلومات ذات الصلة، حول أمن أنظمة المعلومات والشبكات والبيانات إلى الأطراف المعنية، وذلك بهدف توفير فهم للحالة الأمنية والمخاطر الحالية وتدابير الحماية المتخذة، بالإضافة إلى إجراءات التخفيف المخطط لها.

وتكمن أهمية الإفصاح عن المخاطر السيبرانية في إظهار جميع المعلومات الضرورية وتلبية احتياجات مستخدمي القوائم المالية، لمساعدتهم في اتخاذ القرارات، وتخفيض حالة عدم التأكد (يوسف، ٢٠٢٢، ص٤٨-٤٩). ويخصص السوق قيماً سوقية أعلى للشركات ذات الجودة العالية لإفصاحات الأمن السيبراني (Berkman et al., 2018). وأن الارتباط الإيجابي بين الإفصاح عن الأمن السيبراني وجاذبية الاستثمار يعتمد على الإفصاح عن مسؤولية الإدارة العليا (Tan & Yu, 2018). ويمكن أن يؤثر بشكل مباشر على ممارسات التقارير المالية للشركات وتصورات أصحاب المصلحة (Walton et al., 2021, p178). ويمكن القول بأن الإفصاح عن المخاطر السيبرانية، هوسيف ذوحدين، لأنه يعمل كحلقة وصل بين المديرين وأصحاب المصلحة لتقليل مستوى عدم تماثل المعلومات، وقد يؤدي إلى جذب المتسللين إلى أنظمة معلومات المنشأة وزيادة احتمالية وقوع حوادث سيبرانية مستقبلاً (Walton et al., 2021, p156; Jiang et al., 2022, p153). ومن منظور الوكالة، يعمل الإفصاح عن المخاطر السيبرانية على التخفيف من عدم تماثل المعلومات بين الإدارة والمساهمين (Al Amosh & Khatib, 2024, p4).

ويمكن أن يكون الإفصاح عن المخاطر السيبرانية أحد الأدوات لبناء صورة إيجابية للمنشأة من شأنها أن تزيد من أرباح المنشأة (Sofiani et al., 2024, p2). وفيما يتعلق بالإفصاحات المرتبطة بالمخاطر السيبرانية، فإن المعلومات التي تكون محددة بدقة، وقابلة للقياس الكمي، وقابلة للتحقق تُعتبر ذات جودة أعلى، لأنها توفر فهماً أوضح وأكثر موثوقية للمخاطر المطروحة (Singh, 2024, p4). ويساعد الإفصاح الشفاف والشامل عن المخاطر السيبرانية في بناء الثقة مع أصحاب المصلحة، ويساعد على زيادة المواقف في السوق، وجذب الاستثمارات، وتخفيف الآثار السلبية للتهديدات لسيبرانية ( Guohong et al., 2025, p6).

**ويرى الباحث أن الإفصاح عن المخاطر السيبرانية هوالقدرة على توفير المعلومات لوصف المخاطر السيبرانية، وحوكمة إداراتها والإستجابة لها وتخفيفها في التقرير السنوي، وبيان أثارها الاقتصادية المتوقعة على الأداء الحالي والمستقبلي، لتقليل درجة عدم التأكد الذي يحيط بتقديم المنشأة للخدمات الرقمية المختلفة.**

وتتمثل طبيعة وخصائص الإفصاح عن المخاطر السيبرانية في؛ أنه ينبغي أن يشارك المحاسبون في تحديد وقياس تكاليف أحداث الأمن السيبراني؛ وتتبع أثر هذه الأحداث (Serag & Daoud, 2022, p21-22). وقدمت بعض الدراسات المحاسبية مثل (Stein,2018; Gao et al.,2020, Eijkelenboom, & Nieuwesteeg, 2021; Haavisto & Suomi, 2024, p50-52) المكونات الرئيسية للافصاح عن المخاطر السيبرانية، وارتكزت على مجموعة من المعايير التي تحدد خصائص الإفصاح من حيث طبيعته ونوعه ونطاقه وتوقيته وطريقته، وذلك وفق الأطر والمتطلبات التي وضعتها (SEC, 2011; SEC, 2018; AICPA, 2017 ;CPA, 2017; CSA, 2018)، والتي شملت ما يلي:

**١/١- طبيعة الافصاحات (النوعية أوالكمية):** إن رأى كل من (SEC, (2011, 2018 AICPA, (2017)؛ أن الافصاح عن المخاطر السيبرانية بشكل عام هوإفصاح غير مالي، وقد يتضمن المحتوى المعلوماتي للتقرير إفصاحاً كمياً (مثل قيمة الاستثمارات في الأمن السيبراني – قيمة الخسائر المتوقعة الناتجة عن المخاطر السيبرانية- قيمة التعويضات والمخصصات لمواجهة الخسائر المحتملة – الخ)، بينما تشتمل الإفصاحات الوصفية على (وصف للمعلومات والأنظمة الحساسة المعرضة للهجوم- وصف لبرنامج إدارة الأمن السيبراني – هياكل إدارة الأمن السيبراني – إلخ). ويشكل الإفصاح عن المخاطر السيبرانية من حيث النوعية والكمية اتجاهاً جديداً في البحث المحاسبي، ويحفز على التفكير فيما إذا كان الإفصاح عن المخاطر السيبرانية يمكن أن يكون قراراً ذا صلة بالقيمة، وتظهر الدراسات السابقة أن جميع المنشآت في كافة القطاعات عرضة للمخاطر السيبرانية (Peng & Li, 2022, p456). وكذلك أكدت دراسة (مطر، (٢٠٢٤، ص٩) على أن الافصاح والتقرير عن المخاطر السيبرانية يعد إفصاح غير مالي.

وإن الإفصاحات المتعلقة بالأمن السيبراني، هي معلومات نوعية وكمية حول سياساتها وتدابيرها واستراتيجياتها المتعلقة بالأمن السيبراني، على سبيل المثال: الخطوات المتخذة للتخفيف من المخاطر التي تم تحديدها، مثل الاستثمارات في التقنيات الجديدة، أوتدريب الموظفين، أوالشراكات مع مقدمي خدمات الأمن السيبراني، والمعلومات حول هياكل الحوكمة، والامتثال للمعايير، ودور مجلس الإدارة في الإشراف على الأمن السيبراني (Bek-Gaik & Surowiec, 2024, p1523).

**٢/١- نوع الإفصاح (الاختياري أوالإلزامي):** ترى دراسة (Gordon et al., 2018) أن المنشآت التي أفصحت عن الأمن السيبراني اختيارياً تتمتع بقيم سوقية أعلى، وتقلل من عدم تماثل المعلومات. وأن ٨٧% من المنشآت الهولندية أفصحت عن الأمن

السيبراني في تقريرها السنوي لعام ٢٠١٨، على الرغم من عدم وجود التزام قانوني ملزم للقيام بذلك (Eijkelenboom &Nieuwesteeg, 2021).

ووفقاً للتوجيهات المقدمة من (AICPA, 2017) و(SEC, 2011, 2018; 2023)، يتعين على المنشآت تقديم إفصاح اختياري حول الأمن السيبراني وإدارة مخاطره. وفي السياق نفسه، تقوم شركات أمريكا اللاتينية أيضاً بدمج الإفصاحات المتعلقة بالأمن السيبراني ومخاطره في تقاريرها السنوية على أساس اختياري (Ramírez et. Al,2022). ومن حيث درجة الإلزام فإنه إفصاحاً اختيارياً (مطر، ٢٠٢٤، ص٩). وقد تفضل المنشآت أيضاً الإفصاح اختيارياً عن معلومات الاختراق للإشارة إلى سوق الأوراق المالية بأن المنشأة تعالج بشكل استباقي قضايا الأمن السيبراني ( Lenka et al., 2023, p175; Gordon et al., 2024, p3).

**وبناءً عليه، يرى الباحث أنه في ظل غياب معايير أوارشادات إلزامية للافصاح عن الأمن السيبراني والمخاطر، يعتبر التقرير عنها إفصاحاً اختيارياً.**

**٣/١- موقع الافصاح عن المخاطر السيبرانية:** على الرغم من أن توجيهات هيئة الأوراق المالية والبورصة لعامي ٢٠١١ و٢٠١٨ أوصت بعدة مواقع يمكن الإبلاغ عن الإفصاح عن المخاطر السيبرانية فيها، إلا أن الموقع الذي تختار فيه المنشآت الإفصاح عن هذه المخاطر لا يزال غير إلزامي (akingump, 2022, p1). وفي مارس٢٠٢٢، أصدرت (SEC) تعديلات لتعزيز متطلبات الإفصاح المتعلقة بإدارة الأمن السيبراني، والافصاح عن الحوادث السيبرانية والتقارير الدورية من قبل المنشآت، لإعلام المستثمرين بشكل أفضل بإدارة مخاطر المنشأة واستراتيجيتها وحوكمتها المتعلقة بالمسائل الإلكترونية، وتقديم إخطار في الوقت المناسب بحوادث الأمن السيبراني الجوهرية، وأرفقت (SEC) هذه الافصاحات بقاعدة تشريعية متمثلة في قانون الأوراق المالية لمخاطر وحوادث الأمن السيبراني الأمريكي (Trautman & Newman, 2022, p7; Ereddia, 2023, p12).

وفي ٢٦ **يوليو٢٠٢٣** اعتمدت (SEC) القواعد النهائية، والتي تتطلب من المسجلين الافصاح عن حوادث الأمن السيبراني الجوهرية، والافصاح الدوري عن المعلومات الجوهرية المتعلقة بإدارة المخاطر السيبرانية واستراتيجية مواجهتها وحوكمتهما في التقارير السنوية، واعتمدت اللجنة أيضاً قواعد تلزم جهات الإصدار الأجنبية الخاصة بتقديم إفصاحات مماثلة، وتتطلب القواعد الجديدة من المسجلين الافصاح في البند (1.05) الجديد من النموذج (8-K) عن أي حادث للأمن السيبراني يعتبرونه جوهرياً، ووصف الجوانب الجوهرية لطبيعة الحادث ونطاقه وتوقيته، بالإضافة إلى تأثيره المادي أوالمعقول، بعد أربعة أيام عمل من تحديد المسجل أن حادث الأمن السيبراني يعد أمراً جوهرياً ( SEC, 2023; Newman et al., 2023, p5).

**وبناءً على ما سبق، يرى الباحث أن يتم الاعتراف بالمخاطر السيبرانية شأنها شأن المخاطر المالية في صلب القوائم المالية إذا أمكن قياسها بدرجة موثوقة، وإذا لم تتمكن المنشأة من قياسها، فينبغي الافصاح عنها في الايضاحات المتممة للقوائم المالية والتقارير السنوية أوتقارير الاستدامة أوالحوكمة أوالتقارير ذات الصلة، وهذا يرجع إلى عدم وجود**

**ارشادات ملزمة للشركات المقيدة بالبورصة المصرية عن الافصاح عن هذه المخاطر، وهذا يتعارض مع وكب التحول الرقمي والشمول المالي والرقمنة.**

**٤/١- توقيت الافصاح عن المخاطر السيبرانية:** بشكل عام، كلما كانت المعلومات أقدم، كانت أقل فائدة (IASB, 2020). ويعد التوقيت عامل مهم في الافصاح عن المخاطر السيبرانية الجوهرية، وأن حوادث الأمن السيبراني، قد لا يتم اكتشافها إلا بعد وقت طويل من وقت حدوثها، وقد تستغرق عواقب الحادث وقتاً لتقييمها بالكامل، وتحديد ما إذا كان الحادث جوهرياً، هوعملية ديناميكية في جميع مراحل اكتشاف وتقييم ومعالجة الحادثة السيبرانية (CSA, 2017b, p5). وقد يقوم المديرون بتعديل توقيت الإفصاح عن مخاطر الأمن السيبراني وإمكانية قراءته وخصوصيته بشكل استراتيجي ( Cheong et al., 2021,p186). وبالنظر إلى الموعد النهائي للإبلاغ خلال أربعة أيام عمل للإفصاح عن حوادث الأمن السيبراني الجوهرية، يجب على المنشآت تقييم ضوابط الإفصاح والإجراءات المرتبطة بتوقيت المخاطر والحوادث السيبرانية والإبلاغ عنها (akingump, 2022, p4). ويمكن للسوق أن يكافئ المنشآت على الشفافية وحسن التوقيت المرتبطين بالإفصاح عن المخاطر السيبرانية (Gordon et al., 2024, p3).

وإن الافصاح الفوري عن الهجوم السيبراني لا يدل على الشفافية والمحاسبة/ المساءلة فقط، بل يسمح أيضاً لأصحاب المصلحة، مثل: المديرين والمستثمرين والعملاء، باتخاذ الاحتياطات اللازمة لمعالجة الموقف وتصحيحه، مما يتيح إدارة المخاطر السيبرانية بشكل أكثر فعالية (Huang et al., 2024, p2). ونظراً لأن عدم تماثل المعلومات يشكل تحدياً لكفاءة السوق وعدالته، فمن الممكن أن يؤدي تأخير الإفصاح عن المخاطر السيبرانية إلى تشويه العمليات العادية للمنشأة التي تعرضت للهجوم (Huang et al., 2024, p3).

وفي هذا السياق، فقد أكدت نتائج دراسة Huang et al., (2024, p4) على ضرورة قيام المنشآت بإعطاء الأولوية لعمليات الافصاح عن المخاطر السيبرانية في الوقت المناسب، وتنفيذ آليات قوية للاستجابة للحوادث، وضمان مشاركة خبرات الأمن السيبراني في صنع القرار الاستراتيجي لحماية رفاهيتها المالية وسمعتها. وبعد الإرشادات المحدثة لـ (SEC)، طبقت قواعد جديدة لتوحيد وإتساق الإفصاح عن المخاطر السيبرانية خلال أربعة أيام عمل، وتقديم إفصاحات سنوية عن حول إدارة هذه المخاطر واستراتيجيات مواجهتها ( Kuli, 2025, p5).

**ويستنتج الباحث أن حسن التوقيت للافصاح عن المخاطر السيبرانية، يوفر المعلومات في الوقت** المناسب، **ويزيد من ثقة العملاء والمستثمرين، وزيادة عدالة وشفافية التقارير المالية للمنشأة، ويعطي إشارة للسوق، بأنها تتمتع بمرونة سيبرانية ملاءمة، وأن المنشأة قادرة على درء المخاطر السيبرانية والتعامل معها.**

**٥/١- حجم الإفصاح عن المخاطر السيبرانية:** إن حجم الإفصاح عن الأمن السيبراني والمخاطر المرتبطة به، قد يتسبب في تعرض المنشأة لتلك المخاطر أوقد تتجنبها، لذلك في بعض الحالات قد يؤدي الإفصاح المفرط عن المخاطر إلى جعل المنشأة أكثر عرضة للهجمات السيبرانية، وعلى الرغم من أن زيادة الإفصاح قد يقلل من مخاطر التقاضي الناتجة

عن الانتهاك، وبالتالي، إذا اكتشفت المنشأة مخاطر جوهرية، فقد تفصح بإيجاز عن مجالات الضعف في الفضاء السيبراني باستخدام لغة نموذجية لا توفر في الحقيقة معلومات مناسبة، أويمكنها تركيز إفصاحها على المخاطر الجوهرية التي تواجهها المنشأة بالفعل، ويعتقد أن الطبيعة النوعية للإفصاح عن المخاطر السيبرانية، تعطي المديرين الفرصة لمناقشة المخاطر السيبرانية بطريقة متفائلة أومتشائمة (Song et al., 2020; Ramírez et al., 2022).

٢- **مزايا وتحديات الافصاح عن المخاطر السيبرانية:** يهدف الإفصاح عن المخاطر السيبرانية إلى توفير معلومات دقيقة لأصحاب المصلحة حول مستوى ونطاق المخاطر السيبرانية (Cheong et al., 2021, p185). وأشارت نتائج دراسة (Wu et al., (2024, p3 إلى أن عواقب الإفصاح عن الأمن السيبراني تعتمد على فهم واضح لمحتوى المعلومات في الإفصاح عن الأمن السيبراني. ويمكن تحليل مزايا وتحديات الافصاح عن المخاطر السيبرانية على النحوالتالي:

**١/٢- مزايا ومنافع الافصاح عن المخاطر السيبرانية:**

يمكن للمنشآت من خلال استخدام تدابير الإفصاح عن المخاطر السيبرانية، مقارنة مستوى المخاطر السيبرانية لديها مع المنشآت التي تنتمي لنفس الصناعة، مما قد يحفزهم على تقليل نقاط الضعف الأمنية لديهم لتحسين أدائهم وجذب المستثمرين (Gao et al., 2020, p2). ويتم استخدام الإفصاح عن المخاطر السيبرانية في التقرير السنوي كمرجع للنظر فيه من قبل المستثمرين عند اتخاذ قرارات الاستثمار، وهذا يوضح مدى أهمية شفافية المعلومات في التقرير السنوي للمنشأة، ولذلك يعد الإفصاح عن المخاطر السيبرانية وإدارتها مهماً لأن المعلومات لها قيمة يمكن أن تجعل السوق يتفاعل بشكل أفضل (Sofiani et al., 2024, p2).

ووفقاً **لنظرية الشرعية**، ستستخدم المنشآت عمليات الإفصاح عن المخاطر السيبرانية لمحاولة استعادة ثقة المستثمرين والمصداقية من خلال تحمل المسؤلية عن الخرق، وتقديم رؤية صادقة وشفافة لعمليات الأمن السيبراني للمنشأة (D'Arcy & Basoglu, 2022, p784) . وبناء الثقة لتوفير الشفافية حول كيفية وفاء مجالس الإدارة بمسؤولياتها في الإشراف على المخاطر السيبرانية، لتحقيق المرونة السيبرانية (Klemash et al., 2020, p1; Slapničar, 2023, p4). ويوفر الإفصاح عن المخاطر السيبرانية في التقرير السنوي فرصة للإشارة إلى الأسواق التي تشارك فيها المنشأة في منع واكتشاف وتصحيح الفجوات المتعلقة بالأمن السيبراني (Ehioghiren & Ojeaga, 2021, p21).

وتساعد عمليات الافصاح عن المخاطر السيبرانية وسياسات الإدارة البارزة والشاملة والمتكررة على غرس الثقة في الأشخاص بشأن المنشأة (Lenka et al., 2023, p175, 176). وقد تمارس الإفصاحات عن المخاطر السيبرانية دوراً مهماً في إرسال إشارات إلى أصحاب المصلحة حول درجة وعي الإدارة بقضايا الأمن السيبراني، التي تتخذها لحماية المنشأة وتحديد التهديدات والاستجابة لها بشكل مناسب (Singh, 2024, p4).

**٢/٢- تحديات الافصاح عن المخاطر السيبرانية:**

لا يزال الإفصاح عن المخاطر السيبرانية على الرغم من اكتسابه الاهتمام، يواجه العديد من التحديات، ويمكن تلخيصها فيما يلي (Lee, 2018, p8-10; Zukis, 2022; Von Skarczinski et al., 2022, p3-4; Haavisto & Suomi, 2024, p17) :

١- **صعوبة الوصول إلى بيانات موثوقة:** من الصعب الحصول على معلومات مفصلة عن الانتهاكات الأمنية من المنشآت المتضررة بسبب حساسيتها والتأثير السلبي المحتمل لنشرها، وقد تؤدي البيانات غير المكتملة، إلى حجب الإفصاح العلني عن الأخبار السلبية، وتجنب المشاكل المالية المستثمرين.

٢- **التحديات الراهنة من الناحية العملية**: وتتمثل في(عدم وجود معايير أومبادئ توجيهية أوسياسات واضحة بشأن ما يجب الإفصاح عنه، ومتى ينبغي الإفصاح عنه، ومن خلال القنوات التي ينبغي أن يتم الإفصاح عنها، وعدم وجود معايير يمكن أن تستخدم كمؤشرات أومقاييس للامتثال للإفصاح).

٣- **التحديات التي تواجه صانعي السياسات: وتتمثل في: احتياجات أصحاب المصلحة من المعلومات**: حاجة الجمهور إلى معلومات كافية؛ **وحسن التوقيت:** لتزويد الطرف المتضرر في الوقت المناسب بالمعلومات المتعلقة بالانتهاك، **والشفافية:** الحاجة إلى اتصالات واضحة لا لبس فيها بعد خرق أمني، **والتنفيذ:** فرض قدر أكبر من الالتزامات القانونية بحيث تكون الجزاءات والعقوبات المناسبة معروفة بشكل أفضل.

٤- **ارتفاع تكاليف الإفصاح وتزويد المهاجم بالمعلومات**: هناك أيضاً تكاليف مرتبطة بالإفصاح عن المخاطر السيبرانية في التقارير السنوية، فمن ناحية **التكاليف الإدارية** لتجميع المعلومات المتعلقة بتدابير الأمن السيبراني (Eijkelenboom & Nieuwesteeg, 2021, p5). **ومن ناحية أخرى**، قد يؤدي إلى زيادة احتمالية وقوع هجمات سيبرانية مما قد يؤدي إلى التقاضي وخسائر التشغيل في المستقبل (Wang et al., 2022, p3.

لذلك، واستناداً إلى نظرية تكاليف الملكية، يتم تحفيز المنشآت على الافصاح اختيارياً عن المعلومات ذات الصلة إلى السوق، وذلك من أجل تقليل عدم تماثل المعلومات، فقد تتردد المنشآت في الافصاح عن المعلومات المتعلقة بالأمن السيبراني للجمهور لحماية نفسها من هذه المشكلات (Dye, 1985; Ahsraf & Sunder, 2023; Firoozi & Mohsni, 2024, p10).

**ويرى الباحث أنه يمكن مواجهة تلك التحديات، من خلال الموازنة بين التكاليف والعائد مع مراعاة الشفافية، وفي ذات الوقت مراعاة السرية عندما يكون هناك ضرر حتمي سيلحق بالمنشأة، ويمكن أن يساعد في تحقيق تلك الموازنة إصدار مزيد من المعايير المحاسبية في مجال القياس والإفصاح عن المخاطر السيبرانية، مع الحرص على الإفصاح عن المخاطر السيبرانية الهامة والمؤثرة.**

## المحور الثالث: مؤشر الإفصاح المقترح عن المخاطر السيبرانية وحوكمة إدارتها:

يعد الإفصاح المحاسبي عن المخاطر السيبرانية من المجالات البحثية التي نالت حيزاً واسعاً. حيث أوضحت دراسة Li et al., (2018, p30) أن الوحدات الاقتصادية تعمل على الإفصاح عن المخاطر السيبرانية، من خلال تقرير مناقشات الإدارة بشكل وصفي، لإعطاء إشارات إيجابية لأصحاب المصالح أن الوحدة الاقتصادية قد أسهمت في إدارة المخاطر السيبرانية، وأنها أفصحت عن جهودها في ذلك من خلال الإفصاح النوعي في أحد تقاريرها السنوية، وبالتالي تعطي صورة مشرقة بأنها كانت استباقية في حفاظها على أمن المعلومات وتقليل حالات الهجمات السيبرانية. ووفقاً لنظرية الإشارة، فإن الإفصاح عن المخاطر السيبرانية يرسل إشارات إيجابية حول الجهود المبذولة في مجال الحماية من المخاطرالسيبرانية، والحد من ظاهرة عدم تماثل المعلومات، مما يمكن المستثمرين من تقييم قدرة المنشأة من الحفاظ على أمنها وتقليل احتمالات حدوث المخاطر السيبرانية، مما ينعكس إيجابياً على تحسين الأداء المالي للمنشأة (علي & علي، ٢٠٢٢، ص ١٢).

فضلاً عن أن الافصاحات الاختيارية تمثل أحد أهم المتطلبات التي ازدادت الدعوات لها من قبل الهيئات المهنية والأطر المحاسبية، فالإفصاح عن المخاطر السيبرانية يسهم في اتجاه التأثير الإيجابي على قرارات المستثمرين (Yang et al., 2020, p167). ويسهم في اتجاه ثقة أصحاب المصالح، وينعكس على جودة القرارات في ظل الصناعات التي تعاني من مخاطر الهجمات سيبرانية (Kelton & Pennington, 2021, p135). وأن الإفصاح في القوائم المالية يتأثر بالحوادث السيبرانية والمخاطر الناتجة عنها على القوائم المالية، حيث يمكن أن تؤدي إلى: (زيادة المصروفات المتعلقة بالتحقيق والإخطار بالاختراق وكيفية علاجها وإمكانية التقاضي، وانخفاض الإيرادات، والمطالبات المتعلقة بالضمانات وعدم الوفاء بالعقد والتعويضات، وانخفاض التدفقات النقدية المستقبلية أواضمحلال الأصول غير الملموسة وغيرها من الأصول، فضلاً عن الاعتراف بمزيد من الالتزامات وزيادة تكاليف التمويل (الرشيدي & عباس، ٢٠١٩، ص ٤٦٢؛ يعقوب وآخرون، ٢٠٢٢، ص١٤١٣-١٤١٤).

واقترح مجلس التقارير المالية (FRC) لمواجهة التحديات التي تواجه المنشآت، من خلال بعض مجالات الافصاحات والاقتراحات التي تتوافق مع احتياجات المستثمرين ويقدرونها، ونقاط المناقشة الداخلية للشركات، وأنواع الإفصاح المتعلقة بكليهما والمتعلقة بـ (استراتيجية الأمن الرقمي، والحوكمة، والمخاطر الرقمية، والأحداث السيبرانية)، وعند تحديد الإفصاحات التي يجب تقديمها، يجب مراعاة الأهمية النسبية للمنشأة والحساسية المحتملة للمعلومات، وما إذا كانت توفر معلومات كافية للمستخدمين (FRC, 2022, p4).

**ويري الباحث أن استجابة المنشآت للإفصاح عن المخاطر السيبرانية، يعد الركيزة الأساسية للحفاظ على الثقة ومصداقية التقارير المرافقة للتقارير المالية (دورياً/ سنوياً)، ولهذا يتطلب الأمر إرساء إطاراً يتضمن مجموعة من الآليات، التي يمكن من خلالها أن**

**تستعين به المنشآت المدرجة في البورصة للإفصاح عن المخاطر السيبرانية وحوكمة إدارتها.**

## ١- بناء هيكل المؤشر المقترح للإفصاح عن المخاطر السيبرانية وحوكمة إدارتها:

على الرغم من أن الدراسات السابقة المتعلقة بالإفصاح عن المخاطر السيبرانية، قد استخدمت في الغالب حساب عدد الكلمات والجمل والتحليل النصي، فقد اختار الباحث في هذه الورقة بناء مؤشر مقترح لإفصاح المنشآت عن المخاطر السيبرانية بما يتلاءم مع البيئة المصرية. وأكدت دراسة Hassan & Marston, (2019) على أن قياس الإفصاح عن المعلومات عن طريق حساب عناصر البيانات ليس حلاً مرضياً لمشكلة الورقة، نظراً لوجود تكرار لبعض البيانات والكلمات في التقارير السنوية. ويؤكد الباحث بأنه بتحليل واستعراض الدراسات السابقة، اتضح أن تحليل المحتوى هوالمنهجية السائدة، بغض النظر عن الأسلوب المستخدم لجمع المعلومات، وتم عرض استخدامه في تقييم إفصاحات الأمن السيبراني ومخاطره في دراسات كل من (يعقوب وآخرون، ٢٠٢٢؛ مسعود & عبدالفتاح، ٢٠٢٤؛ Berkman et al., 2018; Bodin et al., 2018; Li et al.,2018; Skinner, 2019; Gao et al., 2020; Héroux & Forting, 2020; Heidenborg & Lappalainen, 2021; Eijkelenboom & Nieuwesteeg, 2021; Radu & Smaili, 2022; Sebastian, 2022 ; Ramírez et al., 2022; Schubert, 2023; Ereddia, 2023; Uddin et al., 2023; Karyani et al., 2023, p302, 303; Calderon& Gao , 2023; Haavisto & Suomi, 2024, p33- 47; Firoozi & Mohsni, 2024; Cao et al., 2024;Guohong et al., 2025, p7). والتي قطعت شوطاً في هذا المجال.

ويعتبر مؤشر الإفصاح هوأحد الأساليب الرئيسية لتقييم شفافية المعلومات في المنشآت، حيث إنه من عام ١٩٦٠ حتى الوقت الحاضر، كان مؤشر الإفصاح أداة بحث استمرت بمرور الوقت، وتمثل قوائم واسعة من العناصر المختارة التي يمكن الإفصاح عنها في تقارير المنشأة (Hassan & Marston, 2019). وإن بناء مؤشر للإفصاح هوممارسة واسعة الانتشار؛ ويعد تفصيله جزءاً من جانب واحد من منهجية تحليل المحتوى، وتؤكد الدراسات السابقة المتعلقة بقضايا الإفصاح عن معلومات المخاطر السيبرانية قبولها الواسع في الدراسات المحاسبية. وتقوم هذه الدراسات في الغالب بتقييم المعلومات المفصح عنها بشأن المخاطر السيبرانية من قبل المنشآت المدرجة في التقارير المقدمة إلى لجنة الأوراق المالية والبورصات (Ramírez et al., 2022, p9).

وقام عدد من الدراسات المحاسبية، بتحليل المحتوى المتعلق بالمخاطر السيبرانية التي تم الإفصاح عنها في التقارير السنوية، وعلى سبيل المثال، فحصت لجنة الأوراق والبورصات الكندية (CSA, 2017b) ممارسات الإفصاح الخاصة بـ ٢٤٠ منشأة تتألف من مؤشر S & P/ TSX المركب، وأبلغت عن توقعاتها فيما يتعلق بالإفصاح عن عوامل المخاطر

(الإفصاح عن المخاطر السيبرانية، والتأثيرات المحتملة لحادث الأمن السيبراني، والحوكمة، وتخفيف المخاطر السيبرانية)، والإفصاح عن حادثة الأمن السيبراني الفعلية، وتوصلت إلى أن المنشآت تستخدم لغة معيارية في الإفصاح عن المخاطر السيبرانية Héroux & (Fortin, 2020, p80). واستخدمت بعض الدراسات المتعلقة بإفصاحات الأمن السيبراني تحليلاً نصياً للغة، استناداً إلى إفصاحات المنشآت في النموذج (10-K)؛ وطور كل من Gordon et al., (2018); Berkman et al., (2018) مؤشراً يحدد وجود إفصاحات طوعية تتعلق بالأمن السيبراني ؛ والنتائج التي توصلوا إليها تدعم بشكل عام أهمية التأكيد عن الإفصاح عن المخاطر السيبرانية.

ويستعرض الباحث بعض الدراسات السابقة، والتي اقترحت مؤشر للإفصاح عن المخاطر السيبرانية، فالأولى تم إعدادها بناءً على إرشادات المنظمين الماليين للشركات المدرجة في مؤشر (S&P/TSX 60) لبورصة تورنتو(TSX) بكندا، وتكون المؤشر من (٤٠) بند، ومقسم لسبع فئات هي: (١) المخاطر المرتبطة بالأمن السيبراني (٤بنود)، (٢) الآثار المحتملة للحوادث المرتبطة بالأمن السيبراني (١١بند)، (٣) المسئولية المرتبطة بوضع الإستراتيجيات المتعلقة بالأمن السيبراني (٦بنود)، (٤) تخفيف المخاطرالسيبرانية (١١بند)، (٥) الحوادث السيبرانية المحتملة (بندين)، (٦) الحوادث السيبرانية الفعلية (٣بنود)، (٧) بنود الأمن السيبراني الأخرى التي تم الإفصاح عنها (٣بنود) ( CSA, 2017b; Héroux & Fortin, 2020).

في حين قامت شركة EY, (2018; 2019;2020; 2021) الدولية، بتحليل إفصاحات المخاطر السيبرانية في (10-K) لشركات (Fortune 100)، وتتألف أداة القياس من (٢٣) عنصر، ومقسم لثلاث فئات، وهي: إشراف ورقابة مجلس الإدارة (مدخل مراقبة المخاطر) (١)، الإشراف على لجنة المخاطر من قبل مجلس الإدارة (٣)، مهارات المدير وخبراته (٢)، وهيكل التقارير الإدارية (٢)، وتكرار تقارير الإدارة (٢) ؛ وبيانات المخاطر السيبرانية (الإفصاح عن عوامل الخطر (٢) ؛ إدارة المخاطر السيبرانية (جهود إدارة المخاطر السيبرانية (٦)، والتعليم والتدريب (١)، والتعامل مع المجتمع الأمني الخارجي (١)، وتعيين مستشار خارجي مستقل (٣). وتم قياس الإفصاح عن المخاطر السيبرانية في دراسة Cheong et al., (2021) وتم تطبيقها على ٤٩١٨ منشأة بالولايات المتحدة الأمريكية، وذلك من خلال تطبيق التحليلات النصية، وتصنيفها إلى تسعة عوامل تم وصفها على النحوالتالي: (السيطرة على الحوادث وتخفيف المخاطر، والمخاطر التشغيلية، والمتعلقة بالعملاء، والمتعلقة بالعقود، واستمرارية الأعمال، ونظام الدفع، وأمن الشبكة، ومقدمي برامج الأطراف الثالثة، والتأكيد).

وتم بناء مؤشر الإفصاح عن المخاطر السيبرانية، وفقاً لدراسة Heidenborg & Lappalainen, (2021) من (٨) بنود رئيسية في تقارير المخاطر السيبرانية لأكبر المنشآت الدولية، والتي اتخذت من أوربا مقراً لها، وهي: (١) أنواع المخاطر، و(٢) عواقب المخاطر (المحتملة أوالمحققة)، و(٣) التخفيف من حدة المخاطر و(٤) الحوادث السيبرانية (وصف وتحليل الحوادث السيبرانية التي حدثت بالفعل)، و(٥) نطاق المعلومات (المعلومات

المتعلقة بالمنشأة أوبالمنشآت بوجه عام)، و(٦) التوجه الزمني (التركيز على الماضي أوالمستقبل فيما يتعلق بإستراتيجية الأمن السيبراني)، و(٧) ملاءمة الوقت للمخاطر، و(٨) الغموض (تفاصيل قليلة وتفسيرات موجزة). وتمت دراسة (يعقوب وآخرون، (٢٠٢٢) بالبيئة العراقية، وتكون المؤشر المقترح من خمس أبعاد (٣٣ بند)، وهي: حوكمة الأمن السيبراني (١٠) بنود، وحماية الأمن السيبراني (٦) بنود، والاستراتيجية (الرؤية المستقبلية) (٥) بنود، وإدارة المخاطر السيبرانية ويتضمن (٤) بنود، والاثار المالية ويتضمن (٨) بنود. وأخيراً، طبقت دراسة Firoozi & Mohsni, (2024) على ١٢٠ منشأة تنتمي لـ ٦ قطاعات (بواقع ٢٠ منشأة لكل قطاع) بإجمالي مشاهدات (٨٤٠) مشاهدة في بورصة تورونتوضمن مؤشر (TSX) بكندا، وتم بناء مؤشر الإفصاح عن الأمن السيبراني من ٦٢ عنصراً، وذلك من خلال تطوير مؤشر يحتوي على ست فئات فرعية، وهي: المخاطر (٩ بنود)، والأثر (١٣ بند)، والحوكمة (٧ بنود)، والتخفيف (١٥ بند)، والحوادث (١٥ بند)، وغيرها (٣ بنود)، ولقياس متغير الإفصاح، قام بحساب الدرجة الإجمالية لكل مشاهدة، والتي تم حسابها على أنها إجمالي عدد العناصر المفصح عنها مقسوماً على إجمالي عدد العناصر التي تنطبق على كل مشاهدة.

**واعتمدت جميع هذه الدراسات على آلية تطبيق المحتوى، ومن خلال تبني مؤشر مقترح للإفصاح عن المخاطر السيبرانية، وتأتي هذه الورقة استكمالاً للدراسات السابقة في مجال بناء مؤشر للإفصاح المحاسبي عن المخاطر السيبرانية، ودراسة إمكانية تطبيقه في البيئة المصرية.**

ولغرض بناء هيكل المؤشر المقترح للإفصاح المحاسبي عن المخاطر السيبرانية وحوكمة إدارتها وسيناريوهات مواجهتها في المنشآت المدرجة بالبورصة المصرية، اعتمد الباحث على ما أصدرته الهيئات المهنية، مثل: (المعهد الأمريكي للمحاسبين القانونيين ( AICPA, 2017). والدليل الارشادي لمعهد المحاسبين القانونين الكندي (CPA.CANDA, 2017) للإفصاح عن المخاطر السيبرانية. وتقرير مجلس التقارير المالية (FRC) الصادر في أغسطس ٢٠٢٢. والدليل الإرشادي لـ (SEC, 2011; 2018). وفي ضوء تكامل إطار COBIT.5، ومعايير الآيزو27001 ISO، وسلسلة NIST SP 800. ومؤشر الإفصاح عن المخاطر السيبرانية لبورصة تورنتو(TSX) الكندية، والمؤشر المقدم من قبل شركة آرنست ويونغ لإفصاحات شركات (Fortune 100) في نموذج (10-K) من ٢٠١٨ حتى ٣١ مايو٢٠٢١ (EY,2018; 2019; 2020; 2021). ومعيار مجلس معايير الاستدامة (SASB). بالإضافة إلى الاستعانة بالاستراتيجية المصرية للأمن السيبراني (٢٠١٧-٢٠٢١). اضافةً إلى التعليمات والأطر والقرارات الصادرة عن الهيئة العامة للرقابة المالية المصرية والبنك المركزي المصري، فضلاً عن بعض الدراسات السابقة، مثل: (يعقوب وآخرون، ٢٠٢٢؛ مسعود & عبدالفتاح، ٢٠٢٤؛ Berkman et al., 2018; Bodin et al., 2018; Li et al.,2018; Skinner, 2019; Gao et al., 2020; Héroux & Forting, 2020; Heidenborg & Lappalainen, 2021; Eijkelenboom & Nieuwesteeg, 2021; Radu & Smaili, 2022; Sebastian, 2022 ; Ramírez

et al., 2022; Schubert, 2023; Ereddia, 2023; Uddin et al., 2023; Karyani et al., 2023, p302, 303; Calderon & Gao ,2023 ; Cao et al., 2024; Firoozi & Mohsni, 2024, p15-17; Haavisto & Suomi, 2024, p33- 47; Guohong et al., 2025, p7).

وتأسيساً على ماسبق، يعرض الباحث بنود مؤشر الإفصاح عن المخاطر السيبرانية في ضوء المعايير والاصدارات المهنية والدراسات المحاسبية ذات العلاقة، من خلال الجدول التالي رقم (٢) :

**جدول رقم (٢)**
**المؤشر المقترح للافصاح عن المخاطر السيبرانية**

| فئات الافصاح | م | بنود الإفصاح | الفترة الحالية | الفترة السابقة | التمييز كمى/ نوعي |
|---|---|---|---|---|---|
| أولاً: قنوات الإتصال الإلكترونية | ١ | ماهية المنشأة وطبيعة أنشطتها. | × | × | نوعي |
| | ٢ | عنوان البريدالإلكتروني (رابط مباشر مع العملاء وشركاء الأعمال) | × | × | نوعي |
| | ٣ | عدد مراكز البيع والفروع الإلكترونية التي تقبل البطاقات أوالدفع الإلكتروني. | × | × | كمي |
| | ٤ | عدد حسابات مشتركي وقيمة المعاملات عبر الإنترنت. | × | × | كمي |
| | ٥ | مدى توافر التطبيقات الإلكترونية الخاصة بالمنشأة . | × | × | نوعي |
| | ٦ | مدى توافر المعلومات عن المنتجات والخدمات الإلكترونية المقدمة من قبل المنشأة . | × | × | نوعي |
| | ٧ | عدد الخدمات المقدمة عبر الموقع الإلكتروني الخاص بالمنشأة . | × | × | كمي |
| | ٨ | سياسة وبرامج المنشأة لحماية البيانات والمعلومات والخصوصية (السرية - السلامة - التوافر). | × | × | نوعي |
| ثانياً: المخاطر السيبرانية الفعلية والمحتملة | ٩ | وصف طبيعة الحوادث والهجمات السيبرانية المحتمل التعرض لها مستقبلاً. | × | × | نوعي |
| | ١٠ | الغرض من الهجمات السيبرانية (التجسس- تعطيل العمليات- التشويش- السرقة والإبتزاز). | × | × | نوعي |
| | ١١ | مصدر الهجمات والحوادث السيبرانية المحتملة. | × | × | نوعي |
| | ١٢ | مخاطر البنية التحتية للمعلومات والخدمات السحابية للعملاء. | × | × | نوعي |
| | ١٣ | مخاطر إساءة إستخدام الممتلكات الفكرية أوالأصول الأخرى (الأجهزة والبرامج والتطبيقات). | × | × | نوعي |
| | ١٤ | مخاطر الإستعانة ببرامج مفتوحة المصدر. | × | × | نوعي |
| | ١٥ | مدي تعرض المنشأة لمخاطر الطرف الثالث، والتغيرات التي حدثت في ذلك التعرض. | × | × | نوعي |
| | ١٦ | مدي تعرض المنشأة لمخاطر وسائل التواصل الإجتماعي | × | × | نوعي |
| | ١٧ | المخاطر التكنولوجية ومخاطر فشل النظام السيبراني. | × | × | نوعي |
| | ١٨ | مخاطر سرية وخصوصية البيانات المخزنة في الفضاء السيبراني. | × | × | نوعي |
| | ١٩ | الإفصاح عن الضوابط والإجراءات الرقابية المرتبطة بالمخاطر السيبرانية. | × | × | نوعي |
| ثالثاً: الآثار المحتملة للمخاطر السيبرانية | ٢٠ | مدى التعرض لتعطيل أوتوقف النشاط / التأخر عن بدء أوتشغيل النشاط (الإيرادات المفقودة). | × | × | كمي/نوعي |
| | ٢١ | مدى التعرض للإضرار بالسمعة/ الميزة التنافسية نتيجة التعرض للحوادث والإختراقات السيبرانية. | × | × | نوعي |
| | ٢٢ | مدى تعرض الأصول غير الملموسة/أوالرقمية المرتبطة بالأجهزة أوالبرامج لإضمحلال القيمة. | × | × | كمي/نوعي |
| | ٢٣ | المبالغ المتكبدة للتعافي من الهجمات السيبرانية السابقة والاجراءات البديلة لضمان استمرار العمل. | × | × | كمي/نوعي |
| | ٢٤ | التقرير عن قياس تكاليف حوادث الأمن السيبراني وعواقبها ومخاطرها. | × | × | كمي |
| | ٢٥ | التأثير على نتائج عمليات التشغيل المستقبلية أوالسيولة أوالوضع المالي للمنشأة . | × | × | كمي |
| رابعاً: حوكمة إدارة المخاطر السيبرانية ومسئولية | ٢٦ | هيكل حوكمة إدارة المخاطر السيبرانية. | × | × | نوعي |
| | ٢٧ | الإطار العام لإدارة المخاطر السيبرانية والإفصاح والتقرير عنها. | × | × | نوعي |
| | ٢٨ | أهداف وسياسات وإجراءات وفعالية الرقابة الداخلية على إصدار التقارير المالية. | × | × | نوعي |
| | ٢٩ | المسؤوليات المذكورة في إستراتيجية الأمن السيبراني للمنشأة، والتغيرات التي طرأت عليها. | × | × | نوعي |

| | | | | | |
|---|---|---|---|---|---|
| مجلس الإدارة | ٣٠ | مسئولية لجنة المراجعة في التقرير والإفصاح عن المخاطر الأمنية وقضايا الأمن السيبراني. | × | × | نوعي |
| | ٣١ | التقرير عن مساهمة الإدارة في تصميم وتقييم نظام إدارة مخاطر أمن المعلومات. | × | × | نوعي |
| | ٣٢ | مسئولية لجنة إدارة المخاطر بشأن المخاطر السيبرانية. | × | × | نوعي |
| | ٣٣ | الإفصاح عن وصف مشاركة المجلس في الإشراف على المخاطر والفرص المتعلقة بالأمن السيبراني. | × | × | نوعي |
| | ٣٤ | الإفصاح عن وصف الأمن السيبراني و/ أومخاطر أمن المعلومات. | × | × | نوعي |
| | ٣٥ | وجود فريق متخصص في إدارة أمن المعلومات والرقابة الأمنية على العمليات الإلكترونية للمنشأة . | × | × | نوعي |
| | ٣٦ | الإفصاح عن تكرار التقارير الإدارية المقدمة إلى مجلس الإدارة أواللجنة. | × | × | نوعي |
| | ٣٧ | الالتزام بالتشريعات والقوانين واللوائح الصادرة عن الجهات المختصة المتعلقة بالأمن السيبراني. | × | × | نوعي |
| | ٣٨ | خبرة مُصدر التقارير والقوائم المالية في مجال تكنولوجيا المعلومات / الأمن السيبراني. | × | × | نوعي |
| خامساً: استراتيجيات تخفيف المخاطر السيبرانية | ٣٩ | مدى وجود خطة واستراتيجية للتعافي من الكوارث / تغطية الحوادث / خطة الإستجابة. | × | × | نوعي |
| | ٤٠ | الإفصاح عن الجهود المبذولة في التعليم والتدريب (الإدارة، والموظفين)، للتخفيف من المخاطر السيبرانية | × | × | نوعي |
| | ٤١ | تكاليف الإستثمار في التكنولوجيا والأدوات الرقمية، والعوائد المتوقعة نتيجة تطبيقها. | × | × | كمي |
| | ٤٢ | الإفصاح عن المعلومات المتعلقة بقياس جهود الأمن السيبراني الجارية. | × | × | نوعي |
| | ٤٣ | مدى إمكانية الإعتماد على الخبراء (طرف ثالث) في مجال الأمن السيبراني. | × | × | نوعي |
| | ٤٤ | مدى توافر معلومات توضح ممارسات المنشأة لحماية وتخزين واسترجاع البيانات إلكترونياً. | × | × | نوعي |
| | ٤٥ | التقرير عن إجراءات الاستجابة للحوادث في نظم المعلومات (خطة الطوارئ/ إختبارات الإختراق). | × | × | نوعي |
| | ٤٦ | عدد الرسائل والتعليمات الإرشادية لتوعية العملاء بالمخاطر السيبرانية عبر موقع المنشأة . | × | × | كمي |
| | ٤٧ | عدد الشهادات التي حصلت عليها المنشأة في الأمن السيبراني/ حوكمة تكنولوجيا المعلومات. | × | × | كمي/نوعي |
| | ٤٨ | الإطر العالمية التي تتبناها المنشأة لحوكمة تكنولوجيا المعلومات. | × | × | نوعي |
| | ٤٩ | الافصاح عن الدورات التدريبية (عددها/ ميالغها) المنعقدة داخل وخارج المنشأة . | × | × | كمي/نوعي |
| | ٥٠ | إتفاقيات ورسوم تجديد التراخيص الأمنية اللازمة. | × | × | كمي/نوعي |
| | ٥١ | الدعم المالي لتطوير البرامج الالكترونية لحماية وتعزيز الأمن السيبراني. | × | × | كمي |
| | ٥٢ | الإحتفاظ بنسخ إحتياطية للمعلومات والسجلات والعمليات الخاصة بالمنشأة وتحديثها دورياً. | × | × | نوعي |
| | ٥٣ | حجم وعدد عقود الشراكات مع العديد من المنشآت العالمية في مجال الأمن السيبراني. | × | × | كمي/نوعي |

## ٢ـ عناصر المؤشر المقترح للإفصاح عن المخاطر السيبرانية وحوكمة إدارتها:

يتكون المؤشر المقترح من المحاور الخمس التالية، وهي: قنوات الاتصال الإلكترونية للمنشأة، والمخاطر السيبرانية الفعلية والمحتملة، والآثار المحتملة للمخاطر السيبرانية، وحوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة، وأخيراً، استراتيجيات تخفيف المخاطر السيبرانية، وفقاً للجدول السابق رقم (٧)، وهي كالتالي:-

### ٢/١ـ الإفصاح عن قنوات الاتصال الإلكترونية للمنشأة:

اعتمد الباحث على إطار معهد المحاسبين القانونيين AICPA, (2017) لتبني عناصر هذا المحور، وذلك وفقاً لمعايير الوصف، والتي تتمثل في (١) طبيعة أعمال المنشأة وعملياتها، و(٢) الأنواع الرئيسية من المعلومات الهامة التي يتم تجميعها واستخدامها أوتخزينها بواسطة المنشأة، و(٤) العوامل التي لها تأثير كبير على المخاطر الحتمية للأمن السيبراني، ومن أمثلتها خصائص التكنولوجيا التي تستخدمها المنشأة، والتغيرات البيئية والتكنولوجية والتنظيمية، و(٧) قنوات اتصال الأمن السيبراني، وكذلك اعتمد الباحث أيضاً على دراسة كل من :عقل، زهري، (٢٠٢٠، ص٢٥٥)؛ الفقي، (٢٠٢١، ص٩٣)؛ على، (٢٠٢٢،

ص٤٤٤-٤٤٥؛ Zabala et al., (2020); Florackis et al., (2023, p391-394) في هذا المحور.

ويتضمن الإفصاح عن قنوات الاتصال الإلكترونية (٨) مؤشرات كالتالي: (١) ماهية المنشأة وطبيعتها، و(٢) عنوان البريد الإلكتروني (رابط مباشر مع العملاء وشركاء الأعمال)، و(٣) عدد مراكز البيع والفروع الإلكترونية التي تقبل البطاقات أوالدفع الإلكتروني، و(٤) عدد حسابات مشتركي وقيمة المعاملات عبر الإنترنت، و(٥) مدى توافر التطبيقات الإلكترونية الخاصة بالمنشأة، و(٦) مدى توافر المعلومات عن المنتجات والخدمات الإلكترونية المقدمة من قبل المنشأة، و(٧) عدد الخدمات المقدمة عبر الموقع الإلكتروني للمنشأة، و(٨) سياسة وبرامج المنشأة لحماية البيانات والمعلومات والخصوصية (السرية – السلامة-التوافر).

### ٢/٢ ـ المخاطر السيبرانية الفعلية والمحتملة:

ويتضمن الإفصاح عن المخاطر السيبرانية الفعلية والمحتملة (١١) مؤشر كالتالي: (١) وصف طبيعة الحوادث والهجمات السيبرانية المحتمل التعرض لها مستقبلاً، و(٢) الغرض من الهجمات السيبرانية (التجسس- تعطيل العمليات- التشويش- السرقة والإبتزاز)، و(٣) مصدر الهجمات والحوادث السيبرانية المحتملة، و(٤) مخاطر البنية التحتية للمعلومات والخدمات السحابية للعملاء، و(٥) مخاطر إساءة إستخدام الممتلكات الفكرية أوالأصول الأخرى (الأجهزة والبرامج والتطبيقات)، و(٦) مخاطر الإستعانة ببرامج مفتوحة المصدر، و(٧) مدي تعرض المنشأة لمخاطر الطرف الثالث، والتغيرات التي حدثت في ذلك التعرض، و(٨) مدي تعرض المنشأة لمخاطر وسائل التواصل الإجتماعي، و(٩) المخاطر التكنولوجية ومخاطر فشل النظام السيبراني، و(١٠) مخاطر سرية وخصوصية البيانات المخزنة في الفضاء السيبراني، و(١١) الإفصاح عن الضوابط والإجراءات الرقابية المرتبطة بالمخاطر السيبرانية.

### ٣/٢ ـ الآثار المحتملة للمخاطر السيبرانية:

ويتضمن الإفصاح عن الآثار المحتملة للمخاطر السيبرانية (٦) مؤشرات كالتالي: (١) مدى التعرض لتعطيل أوتوقف النشاط/ التأخر عن تشغيل النشاط (الإيرادات المفقودة)، و(٢) مدى التعرض للإضرار بالسمعة/ الميزة التنافسية نتيجة التعرض للحوادث السيبرانية، و(٣) مدى تعرض الأصول غير الملموسة/أوالرقمية المرتبطة بالأجهزة أوالبرامج لإضمحلال القيمة، و(٤) المبالغ المتكبدة للتعافي من الهجمات السيبرانية السابقة والاجراءات البديلة لضمان استمرار العمل، و(٥) التقرير عن قياس تكاليف حوادث الأمن السيبراني وعواقبها ومخاطرها، و(٦) التأثير على نتائج عمليات التشغيل المستقبلية أوالسيولة أوالوضع المالي للمنشأة.

### ٤/٢ ـ حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة:

ويتضمن الإفصاح عن حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة (١٣) مؤشر كالتالي: (١) هيكل حوكمة إدارة المخاطر السيبرانية، و(٢) الإطار العام لإدارة الأصول السيبرانية والإفصاح والتقرير عنها، و(٣) أهداف وسياسات وإجراءات وفعالية الرقابة الداخلية على إصدار التقارير المالية، و(٤) المسؤوليات المذكورة في إستراتيجية الأمن السيبراني للمنشأة، والتغيرات التي طرأت عليها، و(٥) مسئولية لجنة المراجعة في التقرير والإفصاح عن المخاطر الأمنية وقضايا الأمن السيبراني، و(٦) التقرير عن مساهمة الإدارة في تصميم وتقييم نظام إدارة مخاطر أمن المعلومات، و(٧) مسئولية لجنة إدارة المخاطر بشأن المخاطر السيبرانية، و(٨) الإفصاح عن وصف مشاركة مجلس الإدارة في الإشراف على المخاطر والفرص المتعلقة بالأمن السيبراني، و(٩) الإفصاح عن وصف الأمن السيبراني و/ أومخاطر أمن المعلومات، و(١٠) وجود فريق متخصص في إدارة أمن المعلومات والرقابة الأمنية على العمليات الإلكترونية للمنشأة، و(١١) الإفصاح عن تكرار التقارير الإدارية المقدمة إلى مجلس الإدارة أواللجنة، و(١٢) الالتزام بالتشريعات والقوانين واللوائح الصادرة عن الجهات المختصة أوالجهات الحكومية التشريعية المتعلقة بالأمن السيبراني، و(١٣) خبرة مُصدر التقارير والقوائم المالية في مجال تكنولوجيا المعلومات / الأمن السيبراني.

### ٥/٢ ـ استراتيجيات تخفيف المخاطر السيبرانية:

ويتضمن الإفصاح عن استراتيجيات تخفيف المخاطر السيبرانية (١٥) مؤشر، كالتالي: (١) مدى وجود خطة واستراتيجية للتعافي من الكوارث / تغطية الحوادث / خطة الإستجابة، و(٢) الإفصاح عن الجهود المبذولة في التعليم والتدريب (مجلس الإدارة- جميع الموظفين)، للتخفيف من المخاطر السيبرانية، و(٣) تكاليف الاستثمار في التكنولوجيا والأدوات الرقمية، والعوائد المتوقعة نتيجة تطبيقها و(٤) الإفصاح عن المعلومات المتعلقة بقياس جهود الأمن السيبراني الجارية، و(٥) مدى إمكانية الاعتماد على الخبراء (طرف ثالث) في مجال الأمن السيبراني، و(٦) مدى توافر معلومات توضح ممارسات المنشأة لحماية وتخزين واسترجاع البيانات إلكترونياً، و(٧) التقرير عن إجراءات الاستجابة للحوادث في نظم المعلومات (خطة الطوارئ/ إختبارات الإختراق)، و(٨) الرسائل والتعليمات الإرشادية لتوعية العملاء بالمخاطر السيبرانية عبر موقع المنشأة، و(٩) عدد الشهادات التي حصلت عليها المنشأة في الأمن السيبراني/ حوكمة تكنولوجيا المعلومات، و(١٠) الإطر العالمية التي تتبناها المنشأة لحوكمة تكنولوجيا المعلومات، و(١١) الافصاح عن الدورات التدريبية (مبالغها) المنعقدة داخل وخارج المنشأة، و(١٢) إتفاقيات ورسوم تجديد التراخيص الأمنية اللازمة، و(١٣) الدعم المالي المقدم لتطوير البرامج الالكترونية لحماية وتعزيز الأمن السيبراني، و(١٤) الإحتفاظ بنسخ إحتياطية للمعلومات والسجلات والعمليات الخاصة بالمنشأة وتحديثها دورياً، و(١٥) حجم وعدد عقود الشراكات مع العديد من المنشآت العالمية في مجال الأمن السيبراني.

## المحور الرابع: خلاصة الورقة ومجالات البحث المستقبلية

**خلصت الورقة إلى مجموعة من الدلالات النظرية، والتي يمكن تناولها على النحو التالي:**

- إن الإفصاح عن طبيعة المخاطر السيبرانية وإدارتها، هي إحدى الطرق التي يمكن من خلالها التواصل مع أصحاب المصالح، وينبغي أن تنعكس المخاطر السيبرانية المؤكدة والمحتملة على توفير إفصاحات إضافية للمنشأة في القوائم والتقارير السنوية، وتكمن أهميته في إظهار جميع المعلومات الضرورية وتلبية احتياجات مستخدمي القوائم المالية، لمساعدتهم في اتخاذ القرارات، وتخفيض حالة عدم التأكد، ويكون للمحاسبين دور في قياس تكاليف الحوداث السيبرانية؛ وتتبع أثر هذه الأحداث؛ وضمان قيام المنشآت بالإفصاح عن المخاطر السيبرانية بشكل مناسب، وتحسين عملية إدارة المخاطر السيبرانية لزيادة الثقة والشفافية في التقارير المالية.
- عدم وجود نماذج للإفصاح عن تقرير المخاطر السيبرانية وإدارتها بالمنشآت المقيدة بالبورصة المصرية، وليس هناك نص قانوني يلزمها بذلك، وبالتالي فالمنشآت المقيدة غير ملزمة بالإفصاح عن تقرير المخاطر السيبرانية وحوكمة إدارتها، وبالتالي، وفي غياب معايير أوارشادات إلزامية للافصاح عن الأمن السيبراني والمخاطر، يعتبر التقرير عنها إفصاحاً اختيارياً.
- أكدت الإصدارت والارشادات المهنية للجهات المنظمة لمهنة المحاسبة والمراجعة، على تحسين مناقشة أنشطة الأمن السيبراني في الإفصاحات المالية وتوصيلها بشكل فعال إلى أصحاب المصلحة، كما ركزت الجهات التنظيمية اهتمامها على كيفية معالجة ومراقبة المخاطر السيبرانية في التقارير المالية، وتقديم التقارير إلى مستخدمي البيانات المالية، واتجهت التحديثات الأخيرة نحوالإفصاح عن المخاطر السيبرانية، سواء كانت كمية أونوعية، في تقارير البنوك والشركات.
- استخلصت الورقة البحثية، أنه يتم الاعتراف بالمخاطر السيبرانية شأنها شأن المخاطر المالية في صلب القوائم المالية إذا أمكن قياسها بدرجة موثوقة، وإذا لم تتمكن من قياسها فينبغي الافصاح عنها في الايضاحات المتممة للقوائم المالية والتقارير السنوية أوتقارير الاستدامة أوالحوكمة أوالتقارير ذات الصلة، وهذا يرجع إلى عدم وجود ارشادات ملزمة للشركات المقيدة بالبورصة المصرية عن الافصاح عن هذه المخاطر، وهذا يتعارض مع وكب التحول الرقمي والشمول المالي والرقمنة.
- **مجالات البحث المستقبلية:** بناءً على ما سبق يقترح الباحث المجالات البحثية المستقبلية التالية:

١- نموذج مقترح لقياس أثر الافصاح عن إدارة المخاطر السيبرانية التشغيلية على التكلفة الضمنية لرأس المال وانعكاس ذلك على الأداء المالي للبنوك التجارية المصرية.

٢- أثر الافصاح عن مؤشرات المرونة السيبرانية على الخصائص النوعية لجودة المعلومات المحاسبية وانعكاس ذلك على ترشيد قرارات التعهيد في العصر الرقمي.

٣- أثر القياس والإفصاح المحاسبي عن المخاطر السيبرانية على عدم تماثل المعلومات وانعكاس ذلك على الأداء المالي المستدام بالتطبيق على المنشآت المدرجة بالبورصة المصرية.

٤- نموذج محاسبي مقترح لقياس تكاليف المخاطر السيبرانية للمنتجات الرقمية في ظل تطبيق عقود الشراكة بين القطاعين العام والخاص (BOT) وانعكاس ذلك على ترشيد القرارات الاستثمارية.

٥- الدور المرتقب للمراجع الخارجي في ظل تطور الافصاح عن مخاطر الرقمنة وإدارتها على إعداد تقارير المراجعة الآنية وانعكاس ذلك على تحسين جودة المراجعة المدركة.

## قائمة المراجع

### أولاً: المراجع باللغة العربية:

- **المجلات والدوريات العلمية:**

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

البردونى، ناريمان إسماعيل أحمد. (٢٠٢٥). دور حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني وأثره في تحسين الأداء المالي: دراسة تجريبية على البنوك المقيدة بالبورصة المصرية. مجلة الاسكندرية للبحوث المحاسبية، ٩(١)،١-٧١.

احمد، خالد محمد عثمان. (٢٠٢٣). أثر العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن اجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي – دراسة تطبيقية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، المجلد ١٠، العدد ٤، الجزء الثانى، ديسمبر، ص ١١٠٧-١١٨٣.

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

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

النقودي، سوزي فاروق. (٢٠٢٤). أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، ١١(٤)، ١٦٩-٢١٦.

شحاتة، محمد موسي علي؛ والبردان، محمد فوزي أمين. (٢٠٢١). أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل استراتيجيات الرقمنة على الحد من المخاطر السيبرانية"، المؤتمر الدولي الثالث، الرقمنة وضمان جودة التعليم العالي، جامعة مدينة السادات، ٢-٣ أكتوبر ٢٠٢١، ص١-٢٥.

عبدالله، إيمان السيد محمد.(٢٠٢٤). دراسة العلاقة بين تفعيل ادوات الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية، دراسة تطبيقية علي شركات القطاع العقاري بمصر، المجلة العلمية للبحوث والدراسات التجارية، كلية التجارة، جامعة حلوان، ٣٨(١)، ٦٣-١٠٠.

عثمان، محمد أحمد. (٢٠٢٢). محددات فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، كلية التجارة، جامعة الإسكندرية، ص ١-١٨.

علي، عبد الوهاب نصر. (٢٠٢٤). مسئولية مراقب الحسابات عن كشف الجرائم المالية الإلكترونية (قصور الممارسة ووسائل العلاج). مجلة التجارة والتمويل, كلية التجارة جامعة طنطا، المؤتمر الدولي الثامن لكلية التجارة، جامعة طنطا، عدد خاص ٤٤(٢)، ٢٤٣-٢٦٢.

علي، محمود أحمد أحمد؛ علي، صالح علي صالح. (٢٠٢٢). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية. المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة- تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، (١٠-١١ مارس٢٠٢٢)، كلية التجارة، جامعة الإسكندرية، ص ١-٦٤.

عيسى، عارف محمود كامل؛ محمد، سمير إبراهيم عبد العظيم. (٢٠٢٢). قياس أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحوالإفصاح عن مخاطر الأمن السيبراني: دراسة شبه تجريبية. مجلة الاسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الاسكندرية، ٦ (٣)، ١٢٩-١٩٦.

فرج، هاني خليل. (٢٠٢٢). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني الاستثمار بالأسهم - دراسة تجريبية. مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية، كلية التجارة، جامعة بني يوسف، المجلد ١١، العدد ٢، أغسطس، ص ١٢٩- ٢٠٩.

كعموش، شريف علي خميس ابراهيم. (٢٠٢٤). أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، ١١ (٣)،١-٩١.

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

مسعود، سناء ماهر محمدي؛ عبد الفتاح، هبه بشير الطوخى. (٢٠٢٤). تحليل العلاقة بين خصائص مجلس الإدارة والإفصاح عن مخاطر الأمن السيبراني وأثره على أسعار الأسهم: دراسة تطبيقية علي الشركات المقيدة بالبورصة المصرية. مجلة الأسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الأسكندرية، ٨(١)، ١-٦٢.

مطر، نيفين صلاح على على. (٢٠٢٤). اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان، الدور المعدل لنوع وخبرة مانح الائتمان : دراسة تجريبية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، ١١(٣)، ١-٥٤.

يعقوب، ابتهاج إسماعيل؛ وهاب، اسعد محمد علي؛ الفرطوسى، علي سموم. (٢٠٢٢). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية وفق المتطلبات الدولية: دراسة اختبارية. مجلة الدراسات المالية والمحاسبية والإدارية، كلية الإدارة والإقتصاد، جامعة المستنصرية، مج٩، ع١، ص ١٤٠٣- ١٤٣٠.

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

يوسف، حنان محمد اسماعيل. (٢٠٢٤). القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني – دراسة انتقادية وتجريبية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، ع١، مارس، ص ١-٧٠.

## ثانياً: المراجع باللغة الانجليزية:

Abdelraouf, M., & Hussainey, K. (2025). Systematic review of cyberrisk disclosure practices: insights and implications. The Journal of Risk Finance.

Agarwal, N., Agarwal, S., & Chatterjee, C. (2024). Data Breach Notification Laws and Cost of Debt. The British Accounting Review, 101518.

Asauri, Z. A. F. (2022). Disclosure of Cyber Risk: Its Effect on Banking Profitability in Indonesia(Doctoral dissertation, STIE Indonesia Banking School).

Bansal, G., & Axelton, Z. (2023). Impact of Cybersecurity Disclosures on Stakeholder Intentions. Journal of Computer Information Systems, 1-14.

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

Bek-Gaik, B., & Surowiec, A. (2024). Disclosures on Cybersecurity, Cyber Risks, and Information Security in Non-Financial Reports of Polish Companies. European Research Studies Journal, 27(4), 1513-1535.

Brho, M., Jazairy, A., & Glassburner, A. V. (2025). The finance of cybersecurity: Quantitative modeling of investment decisions and net present value. International Journal of Production Economics, 279, 109448.

Brunner, K. (2025) Quantitative-Automated Risk Consulting in the Cybersecurity Domain. Master Thesis Communication Systems Group (CSG) Department of Informatics (IFI) University of Zurich , Switzerland.

Calderon,T.G.,&Gao, L.(2023).Innovative and Novel Research Datasets Related to Cybersecurity Risk Disclosures: A Research Note. Journal of Information Systems, 37(2),1-6.

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. International Review of Financial Analysis, 93, 103164.

Celeny, D., Maréchal, L., Rousselot, E., Mermoud, A., & Humbert, M. (2024). Prioritizing Investments in Cybersecurity: Empirical Evidence from an Event Study on the Determinants of Cyberattack Costs. arXiv preprint arXiv:2402.04773.

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

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. Journal of Emerging Technologies in Accounting, 20(1), 15-38.

Elnagar, S. M. A., Ahmed, A. S. A. A., & Basiouny, M. M. M. (2024). The Impact Of Cybersecurity Risk Disclosure On The Quality Of Financial Reporting And Market Value. Evidence From Egyptian Stock Market. Educational Administration: Theory and Practice, 30(5), 2504-2516.

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. Future Business Journal, 10(1), 1-15.

Firoozi, M., & Mohsni, S. (2024). Evolution of Cybersecurity Disclosure in Canada. Available at SSRN 4559167.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36 (1) , 351-407.

Gordon, L. A., Loeb, M. P., Zhou, L., & Wilford, A. L. (2024). Empirical evidence on disclosing cyber breaches in an 8-K report: Initial exploratory evidence. Journal of Accounting and Public Policy, 46, 107226.

Harris, D., Kuzey, C., Naaman, C., & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt?. Journal of Forensic and Investigative Accounting, 15 (2).

Histen, M. J. (2022). Taking Information Seriously: A Firm-side Interpretation of Risk Factor Disclosure. International Advances in Economic Research, 1-13.

Huang, J. A., & Murthy, U. (2024). The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions. International Journal of Accounting Information Systems, 54, 100696.

Jiang, W. (2024). Cybersecurity Risk and Audit Pricing—A Machine Learning-Based Analysis. Journal of Information Systems, 1-27.

Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm Use of Cybersecurity Risk Disclosures. Journal of Information Systems, 36 (1) , 151-180.

Khan, W. N., Lee, J. K., & Liu, S. (2025). Is Cybersecurity a Social Responsibility?. Information Systems Frontiers, 1-25.

Khelil, I. (2023). Political connections and cost of debt: a meta-analysis. Journal of Financial Reporting and Accounting,(ahead-of-print).

Li, T., & Walton, S. (2023). Business Strategy and Cybersecurity Breaches. Journal of Information Systems, 1-26.

Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management, 03128962241293658.

Musta'in, A., Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024, July). Cyber Risk Management Disclosure. In Cirebon International Conference on Education and Economics Proceeding (Vol. 1, No. 1, pp. 165-169).

Nelson, A., & Wang, S. (2024). The importance of cybersecurity disclosures in customer relationships. Journal of Corporate Accounting & Finance, 1-9.

Ramírez, M., Rodríguez Ariza, L., & Gómez Mir & a, M. E. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability, 14 (3) , 1390.

Remeis, K. (2023). Board Gender Diversity and Cybersecurity Disclosure Characteristics.

Sari, L., Adam, M., & Fuadah, L. L. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. in 8th Sriwijaya Economics, Accounting, and Business Conference, KnE Social Sciences, 387–398.

Sari, Y. P., Suhardjanto, D., Probohudono, A. N., & Honggowati, S. (2023). Cyber Risk Management Disclosure of State-Owned Enterprises. Journal of Accounting Dynamics, 15(2), 180-190.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. Journal of Forensic & Investigative Accounting, 12 (2) , 197-212.

Wang, X., Li, W. W., Leung, A. C. M., & Yue, W. T. (2024). To alert or alleviate? A natural experiment on the effect of anti-phishing

laws on corporate IT and security investments. Decision Support Systems, 179, 114173.

Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. International Review of Financial Analysis, 103174.