Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. 74, Part (2): 169-187
Doi: www.doi.org/10.25130/tjaes.22.74.2.8

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

Accounting Disclosure Requirements for Cyber Risks in the Information Technology Environment (A Theoretical Study)

Marwa Qutaiba Aldabbagh*, Zeyad Hashim Alsaqa
College of Administration and Economics/University of Mosul

Abstract: This study aims to shed light on the requirements for accounting disclosure of cyber risks in the information technology environment, by analyzing concepts related to accounting disclosure, cyber risks, and their impact on the quality of financial information presented in reports. The importance of the study stems from the escalating volume of cyber threats facing economic entities and the lack of clear disclosure guidelines and treatments related to these risks in the traditional accounting framework.

The study addressed multiple dimensions of disclosure, including: the level of transparency, the timing of disclosure, its location in reports, and its connection to governance and internal control. The study adopted a descriptive and analytical approach, addressing the theoretical aspect through a review of relevant literature, without engaging in field application. The study concluded that there is a noticeable gap in accounting disclosure of cyber risks, due to the absence of a binding regulatory framework, the disparity in disclosure levels among companies, and the lack of awareness among financial departments of the importance of including this information in financial reports. It also recommended the issuance of accounting disclosure standards that address cyber risks, in line with technological developments, to enhance the reliability of reports and the quality of disclosure.

Keywords:
Disclosure requirements, cyber risks.

A R T I C L E I N F O

Article history:

Received	07 Aug. 2025
Received in revised form	07 Aug. 2025
Accepted	10 Aug. 2025
Available online	30 Jun. 2026

*Corresponding author:
Marwa Qutaiba Aldabbagh
College of Administration and Economics/University of Mosul

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. 74, Part (2): 169-187
Doi: www.doi.org/10.25130/tjaes.22.74.2.8

متطلبات الإفصاح المحاسبي عن المخاطر السيبرانية في بيئة تقنيات المعلومات (دراسة نظرية)

مروة قتيبة الدباغ **زياد هاشم السقا**
كلية الإدار ة واقتصاد/جامعة الموصل

المستخلص

يهدف البحث إلى تسليط الضوء على متطلبات الإفصاح المحاسبي عن المخاطر السيبرانية في ظل بيئة تقنيات المعلومات، من خلال تحليل المفاهيم ذات الصلة بالإفصاح المحاسبي، ومخاطر الفضاء السيبراني، وأثرها على جودة المعلومات المالية المعروضة في التقارير. وقد جاءت أهمية الدراسة من تصاعد حجم التهديدات السيبرانية التي تواجه الوحدات الاقتصادية، وافتقار الإطار المحاسبي التقليدي إلى معالجات وإرشادات افصاحية واضحة تتعلق بهذه المخاطر. تناول البحث أبعادًا متعددة للإفصاح، منها: مستوى الشفافية، توقيت الإفصاح، موقعه في التقارير، ومدى ارتباطه بالحوكمة والرقابة الداخلية. واعتمد البحث المنهج الوصفي التحليلي، متناولًا الجانب النظري من خلال مراجعة الأدبيات ذات الصلة، دون الدخول في تطبيق ميداني.

وقد خلص البحث إلى أن هناك فجوة ملحوظة في الإفصاح المحاسبي عن المخاطر السيبرانية، تعود إلى غياب إطار تنظيمي ملزم، وتفاوت مستويات الإفصاح بين الشركات، وضعف وعي الإدارات المالية بأهمية تضمين هذه المعلومات ضمن التقارير المالية. كما توصل البحث إلى ضرورة إصدار معايير إفصاح محاسبي تُعنى بالمخاطر السيبرانية، تتماشى مع التطورات التقنية، بما يعزز موثوقية التقارير وجودة الإفصاح.

الكلمات المفتاحية: متطلبات الإفصاح المحاسبي، المخاطر السيبرانية.

أولاً. مقدمة ومشكلة البحث

يشهد العالم اليوم تحوّلاً جذريًا في بيئة الأعمال نتيجة التوسع المتزايد في استخدام تقنيات المعلومات والاتصالات، مما ساهم في تحسين كفاءة العمليات وتحقيق ميزة تنافسية. إلا أن هذا التحول الرقمي صاحبه تصاعد كبير في المخاطر السيبرانية، التي باتت تهدد استقرار الأنظمة المالية والمحاسبية، وتؤثر بشكل مباشر على مصداقية المعلومات المعروضة في التقارير المالية.

ومع تعقّد الهجمات السيبرانية وتعدد أساليبها، تزايدت الحاجة إلى أن يكون للإفصاح المحاسبي دور فعّال في نقل هذه المعلومات إلى مستخدمي التقارير المالية. غير أن الإفصاح عن المخاطر السيبرانية لا يزال يعاني من غياب إطار محاسبي واضح ومُلزم يُحدد نطاق المعلومات الواجب الإفصاح عنها، وأسلوب عرضها، وتوقيتها، بما يضمن تعزيز الشفافية والمساءلة.

من هنا، تنبع مشكلة البحث من الحاجة إلى معالجة هذا القصور، من خلال دراسة وتحليل متطلبات الإفصاح المحاسبي عن المخاطر السيبرانية في بيئة تقنيات المعلومات، والوقوف على مدى كفأية الأطر المفاهيمية القائمة، والبحث في إمكانية تطوير نموذج إفصاح يدعم جودة المعلومات المحاسبية ويعزز ثقة مستخدميها.

ومن هنا تبرز إشكالية هذا البحث بالسؤال البحثي الآتي"هل يمكن وضع متطلبات للإفصاح المحاسبي عن المخاطر السيبرانية في ظل بيئة تقنيات المعلومات ؟"

ثانياً. هدف البحث: يهدف البحث إلى تحقيق عدد من الأهداف المتمثلة بالآتي:

1. توضيح المقصود بالإفصاح المحاسبي.
2. توضيح المقصود بالمخاطر السيبرانية.
3. تحديد متطلبات الإفصاح المحاسبي عن المخاطر السيبرانية في بيئة تقنيات المعلومات وهو ما يعد الهدف الرئيس للبحث.

ثالثاً. أهمية البحث: تتجلى أهمية هذا البحث في تسليطه الضوء على واحدة من أبرز القضايا المعاصرة في بيئة المحاسبة الرقمية، والمتمثلة في الإفصاح المحاسبي عن المخاطر السيبرانية التي تواجه الوحدات الاقتصادية في ظل الاعتماد المتزايد على تقنيات المعلومات. ففي عصر يشهد تصاعدًا في حجم ونوع الهجمات الإلكترونية، أصبحت الحاجة ملحة لتوفير معلومات مالية وغير مالية شفافة وشاملة تمكّن مستخدمي التقارير من تقييم قدرة الوحدات الاقتصادية على التعامل مع هذه التهديدات، ومدى تأثيرها على الأداء والاستدامة.

وتكمن أهمية الدراسة في كونها تسعى إلى معالجة القصور فيما يتعلق بالإفصاح عن المخاطر السيبرانية في بيئة تقنيات المعلومات.

رابعاً. منهج البحث: اعتمد البحث على الاستنباطي في عرض ومناقشة الدراسات والبحوث والمقالات العلمية المنشورة في المجلات العلمية، وكذلك وضع اساسات نظرية لمتطلبات الإفصاح عن المخاطر السيبرانية في بيئة تقنيات المعلومات.

خامساً. فرضية البحث: في ضوء مشكلة البحث وأهميته وأهدافه يمكن صياغة فرضية البحث من خلال الآتي: "يمكن وضع متطلبات للإفصاح المحاسبي عن المخاطر السيبرانية في ظل بيئة تقنيات المعلومات".

المبحث الأول: ماهية الإفصاح المحاسبي الإلكتروني

أحدثَ الإفصاح الإلكتروني ثورة في مجال الشفافية المالية لكل من المستثمرين والوحدات الاقتصادية المُدرجة في الأسواق المالية مقارنةً مع وسائل الإعلام التقليدية مثل التقرير السنوي الورقي، إذ يسمح الأنترنت للوحدات الاقتصادية بتجميع ونشر أنواع مختلفة من صيغ عرض المعلومات (الفيديو والصوت والنص المكتوب) على مواقع الويب الخاصة بهم. إذ يوفر الإفصاح الإلكتروني للوحدات الاقتصادية الفرصة في تحسين جودة الاتصال، وتحسين السمعة، وجذب المستثمرين المحتملين، وتقليل تكاليف توزيع المعلومات. فضلاً عن أن ظهور شبكة الويب العالمية أدى إلى قيام الوحدات الاقتصادية بإعادة النظر في استراتيجيات الإفصاح الخاصة بها. لأن الويب يوفر مرونة أكبر بكثير من الوسائل التقليدية في عرض التقارير. على سبيل المثال، تقدم مواقع الويب الخاصة العديد من الوحدات الاقتصادية تسهيلات تفاعلية أو توفر الوصول إلى عروض الفيديو. فضلا عن، سماح الويب للوحدة بالإفصاح عن معلومات أكثر بكثير من الوسائل التقليدية يعني هذا السياق أن علاقة الإشراف بين إدارة الوحدة الاقتصادية وحملة أسهُمها تصبح أكثر مباشرة، وديناميكية، وربما تفاعلية، ومن ثم، يتوقع الباحثون من الوحدات الاقتصادية الاستفادة من هذه الفرصة وتنظيم إفصاحها عن المعلومات حول مختلف جوانب أنشطتها في الخارج بِشرط كيف ستفيد المساهمين في النهاية (Cormier et al., 2009: 2).

وعرف الإفصاح المحاسبي الإلكتروني بأنه أحد اشكال النشر الإلكتروني باستخدام موقع الكتروني خاص بالوحدة الاقتصادية يتم من خلاله عرض التقارير المالية والبيانات التوضيحية

بالاستفادة من تقنيات المعلومات الحديثة واستخدام بعض لغات البرمجة (المعيارية) التي تتيح للمستخدم تحقيق أقصى فائدة ممكنة (القزاز والسقا، 2019: 258).

ويستنتج الباحثان ان تعريف الإفصاح الإلكتروني هو النشر الإلكتروني على موقع الوحدة الاقتصادية للقوائم والتقارير المالية والايضاحات الأخرى وتقرير مراقب الحسابات الخاص بهدف التأكد من صحة وسلامة المعلومات المنشورة، وسرعة توصيل واتاحة المعلومات الواضحة والدقيقة لمستخدميها من أصحاب المصلحة، لمساعدتهم في تسهيل عملية اتخاذ القرارات الرشيدة.

ولقد مر الإفصاح الإلكتروني بمراحل عدة فكل مرحلة تختلف عن سابقتها لأنها تقدم آلية جديدة لتلبية المتطلبات الجديدة بهدف زيادة فهم واستيعاب المعلومات من قبل المستخدمين وبناء علاقات ارتباطية بينهم لتقييم وضع الوحدة الاقتصادية.

في بداية التسعينات من القرن الماضي وقبل ظهور الانترنت اعتمدت الوحدات الاقتصادية على ارسال نسخة CD مضغوط تحتوي على المعلومات المالية مرفقة بتقارير مالية ورقية مطبوعة إلى المستفيدين بالبريد، ولكن مع دخول عصر تكنولوجيا المعلومات والانترنت أخذ الإفصاح بالتطور (بيومي، 54:2018)، والآتي المراحل التي مر بها الإفصاح الإلكتروني:

أ. **المرحلة الأولى:** تتمثل هذه المرحلة قيام الوحدات الاقتصادية بتوفير نسخة من المعلومات المالية مطابقة تماماً لتلك المتوفرة في صورتها الورقية من خلال استخدام الورقة الإلكترونية التي من الشائع تسميتها بملف (pdf) وعلى الرغم من المزايا التي يتمتع بها هذا الملف من جودة عالية في الطباعة وانخفاض تكلفة إنتاجهِ وعرضهِ إلا أن هناك بعض السلبيات التي ترافق استخدامه إذ يستغرق وقتاً طويلاً لتحويله كما أنه يفتقد لوجود خاصية الروابط التفاعلية والتي تسمح بالتنقل بين اجزاء التقرير. وكذلك لا يمكن فهرست المعلومات داخل التقرير، فضلاً عن، أن بيانات القوائم المالية لا تكون جاهزة لتحليلها بواسطة المستخدم إذ لا يسمح ملف (pdf) من نسخ القوائم المالية وإعادة تحميلها بصورة جداول الكترونية ليسهل التعامل معها الأمر الذي يتطلب من المستخدم ضرورة إعادة إدخال البيانات مرة أخرى مما يستغرق وقتاً طويلاً (محسن وآخرون، 141:2017).

ب. **المرحلة الثانية:** ظهور لغة البرمجة Hypertext Markup وتستخدم لغة "HTML" كأساس لتصميم مواقع الويب والنصوص التفاعلية في الترميز لعرض معلومات عن المراكز المالية للوحدات الاقتصادية. وهذا يُتيح استخدام الروابط التفاعلية، وهي ميزة غير متوفرة في ملف (pdf)، فضلاً عن امتداد إمكانية فهرسة المعلومات ضمن القوائم المالية، ولكن دورها يقتصر على تقديم معلومات حول كيفية عرض الصفحة دون تقديم أي معلومات حول محتوى البيانات وكيفية تحضيرها. إلى جانب ذلك، فإنه لا يعالج مشكلة تحليل المعلومات التي يواجهها المستخدم عند القيام بذلك. هذا يتطلب إعادة إدخال البيانات كما رأينا في الحالة على ملف (PDF) (Berberi & Benbouali، 2018:43-44).

ج. **المرحلة الثالثة:** تتمثل هذه المرحلة في استخدام الإمكانيات المتطورة لتكنولوجيا الإنترنت وابتكار أشكال عرض جديدة تتجاوز سلبيات المراحل السابقة إذ ظهرت خلال هذه المرحلة لغة الترميز الموسعة(XML)، فتم تبادل المعلومات حول شبكة الإنترنت، وقد صاحب ظهور هذه اللغة اهتمام (Charles) وهو محاسب قانوني يعمل في إحدى الشركات الأمريكية وبدعم وتمويل من قبل المعهد الأمريكي للمحاسبين القانونين بدراسة إمكانية استخدام هذه اللغة في تصميم برنامج لإعداد القوائم المالية الإلكترونية، وبعد محاولات عدة ظهرت لغة تقارير الأعمال الموسعة (XBRL) ويقصد بها برنامج الحاسوب الذي يُضيف بطاقة تعريفية لكل جزيئة من معلومات القوائم المالية الإلكترونية

المُصممة بِاستخدام لغة تقارير الأعمال الموسعة يمكن للمستخدم القيام بإجراء تحليلات للمعلومات دون إعادة معلومات القوائم المالية مرة أخرى كما هو الحال في المراحل السابقة (وفاء وهانية، 2019،7).

تتميز صيغ العرض الرقمية المختلفة (XBRL- HTML-PDF) بخصوصياتها في معالجة المعلومات والتي قد تعيق او تعزز كفاءة المستخدم (صانع القرار) أثناء عملية صنع القرار، إذ لا تسمح صيغة PDF بمعالجة المعلومات مباشرةً، في حين صيغة HTML تسمح بمعالجة المعلومات الثابتة، أما صيغة XBRL فتسمح بمعالجة المعلومات الديناميكية (نورالدين، 2020،54).

في العقد الأخير، تطورت منصات التواصل الاجتماعي في انتاج ونشر معلومات الوحدات الاقتصادية على المنصات، أولاً: معظم منصات التواصل الاجتماعي، تقنيات الوصول المباشر (DAIT) التي تدفع بالمعلومات مباشرة إلى المستخدمين بدلاً من مطالبتهم بالبحث عن المعلومات بشكل استباقي، ثانياً: سمح منصات التواصل الاجتماعي للوحدات الاقتصادية ببدء ونشر المعلومات للمستهلكين في الوقت الحقيقي دون الخروج من خلال وسطاء المعلومات. ونتيجة لذلك، تساعد منصات التواصل الاجتماعي مستخدمي المعلومات على تحديد موقع المعلومات والوصول إليها في الوقت المناسب بتكاليف اقتناء منخفضة، ثالثاً: تسمح مواقع الشبكات الاجتماعي بإنشاء وتبادل المعلومات التي ينشئها المستخدمين على وجه التحديد، يمكن لمستخدمي وسائل التواصل الاجتماعي نشر المعلومات بحرية والرد على المعلومات المقدمة من الوحدات الاقتصادية والمشاركة في تفاعلات متعددة الاتجاهات مع الوحدات الاقتصادية وأصحاب المصلحة الآخرين، بمعنى آخر، لا تأتي المعلومات المُتعلقة بالوحدات الاقتصادية في وسائل التواصل الاجتماعي من الوحدات الاقتصادية فحسب، بل تأتي أيضاً من مستخدمي وسائل التواصل الاجتماعي الآخرين، الذين يلعبون دوراً رئيساً في تشكيل الرأي العام (Lei et al.، 2019: 31).

وقد تَّم تقسيم مراحل تطور الإفصاح الإلكتروني بِواسطة لجنة معايير المحاسبة الدولية International Accounting Standards Committee (IASC) على ثلاث مراحل يمكن تلخيصها على النحو الآتي (رشيد، 2011: 179-180):

1. المرحلة الأولى: تمثلت في إنشاء مواقع الكترونية للوحدات الاقتصادية، استخدام تقنيات الإنترنت كإحدى الوسائل المستخدمة لنشر التقارير المالية من أبرز ملامح هذه المرحلة قلة عدد الوحدات الاقتصادية وعدم انتظام عملية النشر.
2. المرحلة الثانية: تميزت بتزايد عدد الوحدات التي تمتلك مواقع إلكترونية خاصة بها، وتم استخدام هذه التقنية بشكل واسع في نشر التقارير المالية المشابهة إلى حد كبير للتقارير المالية المطلوبة.
3. المرحلة الثالثة: تمثلت هذه المرحلة في زيادة كمية المعلومات المالية وغير المالية المنشورة على الإنترنت بصورة أكبر من التقارير المالية المطبوعة فضلاً عن استخدام طرق مطورة في عرض هذه المعلومات.

وتتمثل أهمية الإفصاح الإلكتروني في اعتقاد منتدى المستشارين في معايير المحاسبة (ASAF) أن التقدم في التقنية يمكن أن يؤدي إلى المزيد من المعلومات التي تصبح جوهرية للمستخدمين. ويرجع ذلك من وجهة نظرهم إلى أن القدرة على استهلاك كميات كبيرة من المعلومات التفصيلية وفهمها بشكل فعال يمكن أن تجعل هذه المعلومات التفصيلية مفيدة، وتتمثل أهمية الإفصاح الإلكتروني بالآتي (سليمان، 2018: 34):

1. تحقق العدالة بين المستثمرين وغيرهم من مستخدمي المعلومات المالية.
2. زيادة درجة الاعتماد على التقارير المالية من قبل مستخدميها في عملية اتخاذ القرارات المالية.
3. زيادة فاعلية الإفصاح لدى الوحدات الاقتصادية من حيث كمية وتمليك المعلومات المعلقة يؤدي إلى ضرورة زيادة فاعلية دورها في اتخاذ القرارات في هذه الوحدات الاقتصادية.

ويرى الباحثان أنه يمكن القول إن الإفصاح الإلكتروني يساعد مستخدمي القوائم المالية في اتخاذ القرارات الملائمة مما يُساعد على تحويل اتجاه الاستثمار والإقراض إلى الوحدات الاقتصادية ذات الكفاءة العالية في استخدام الموارد الاقتصادية المتاحة إليها.

وإن للإفصاح الإلكتروني أهداف عديدة تتمثل بالآتي (سليمان، 199:2018):

1. تسريع عمليات البحث العلمي والتطوير بما يتوافق مع التقنيات التي أفرزتها التقنية الحديثة في المجال المالي.
2. تعميق فرص التجارة الإلكترونية.
3. وضع الإنتاج الفكري لبعض الدول على شكل أوعية الإلكترونية.
4. الإسهام في تصميم المعرفة وإيصالها إلى أي مكان في العالم.
5. توفير خيار الإفصاح ليتواكب مع متطلبات الأجيال الجديدة.
6. تقليص فجوة أزمة الثقة بين المجتمعات العربية وتقنية الإنترنت في مجال الإعلان.
7. المساهمة في صناعة المحتوى الرقمي عربياً وافريقياً على شبكة الإنترنت التي لا تتناسب مع مساهمة الغرب في هذا المجال إذا ما قورنت بمستوى الاستهلاك والاستخدام للمنتجات الرقمية والتقنية في المجتمع العربي.
8. بلورة مفاهيم وقوانين جديدة تتناسب مع متطلبات العصر التقنية.

وإن لاستخدام تقنية المعلومات في المحاسبة أثر ايجابي على تطوير أساليب المحاسبة والإفصاح المالي من خلال تقديم دقيق للبيانات والمعلومات المحاسبية ذات جودة عالية لمستخدمي التقارير المالية، مقارنةً بالإفصاح المحاسبي اليدوي التقليدي وتتمثل مزايا الإفصاح الإلكتروني بالآتي (Benbouali & Berberi, 2018: 42-43):

1. الوفرة في تكاليف طباعة وإرسال التقارير وسرعة النشر التي تشمل المساهمين وحملة السندات الحاليين والمحتملين داخل البلاد وخارجها الذين يتطلعون إلى الاستثمار في الوحدة الاقتصادية.
2. الإفصاح الإلكتروني يحسن الدور الرقابي للمحاسبة من خلال تطوير إمكانية الوصول والتحليل للأرقام المحاسبية لجميع الأطراف المعنية.
3. يدعم استخدام برامج تسمح للمستخدمين بإجراء تحليلات مالية تفاعلية فورية للتواصل مع الوحدات الاقتصادية بتكلفة منخفضة نسبياً.
4. يوفر معلومات ذات شفافية عالية تتصف بالكمال والدقة وسهولة الوصول في الوقت المناسب يوفر الإفصاح الإلكتروني المرونة اللازمة للمستخدمين في البحث والتصفية والاسترجاع والتنزيل وإعادة تكوين هذه المعلومات.
5. يسمح الانترنت بفتح فرص جديدة للإفصاح من خلال محركات البحث والوسائط المتعددة والارتباطات التشعبية.
6. يسهم الإفصاح الإلكتروني في حل مشكلة عدم تماثل المعلومات وآثارها السلبية على المستخدمين، عبر تحقيق الوصول المتكافئ للمعلومات في الوقت المناسب مما يزيد من ثقتهم بالتقارير المالية.

7. يعزز الإفصاح الإلكتروني قواعد حوكمة الشركات في حفظ وضمان حقوق الأطراف كافة.

ويرى الباحثان أن الإفصاح المحاسبي الإلكتروني يمثل حواراً معلوماتياً دائم ومستمر بين الوحدة وأصحاب المصلحة إذ يمكنهم من تقديم معلومات مُصممة خصيصًا لتلبية الاحتياجات.

ولكن يمكن أن يرتبط الإفصاح الإلكتروني بالعديد من العيوب التي قد تمنع الوحدات الاقتصادية من تقديم المعلومات عِبرَ الانترنت لسببين رئيسين هما (عبار، 2022: 53):

أولاً. قد يتم تقييد الممارسات المُؤكدة من خلال مواقف محددة لسلوك الوحدات الاقتصادية مثل نقص ملحوظ في الطلب على الإفصاح، لاسيما في حالة وجود نسبة صغيرة من مستثمري التجزئة.

ثانياً. التكلفة العالية للحفاظ على صفحة علاقات المستثمرين على الانترنت (تكاليف انشاء الموقع، ومراقبة الموقع، والحفاظ على محتوى البيانات، والكشف عن المعلومات للمنافسين، ومخاطر الارتباط التشعبي، ومخاطر التقاضي من المعلومات القديمة.

ولابد من وجود مجموعة من المقومات لإنجاح الوحدات الاقتصادية في تطبيق الإفصاح الإلكتروني وتتمثل هذه المقومات في الآتي (الشطناوي، 293:2018):

1. وجود برامج الكترونية مُتخصصة في إعداد وتشغيل وعرض البيانات.
2. توفير شبكة من الأجهزة والمُعدات الإلكترونية.
3. إنشاء موقع الكتروني للوحدة الاقتصادية على شبكة الإنترنت.
4. وجود إدارة مُتخصصة للموقع الإلكتروني للوحدة الاقتصادية.
5. توافر كوادر بشرية مؤهلة من المُحاسبين والمُبرمجين والمُحللين.
6. إصدار معايير محاسبية تنظم عملية الإفصاح الإلكتروني.
7. استخدام البرامج والأساليب التقنية تؤدي إلى إمكانية التحقق من صحة المعلومات المنشورة، وتوفير التأمين الكافي للموقع.

وهناك عوامل عدة أدت إلى ظهور الإفصاح الإلكتروني، فالتطور الهائل في مجال المعلوماتية وظهور شبكة الإنترنت وتوسعها عِبرَ أنحاء العالم أدى إلى استخدامها في بيئة الأعمال ومع الازدياد المُتنامي لعدد مستخدمي الإنترنت على مستوى العالم وتنوع استخدامات شبكة الإنترنت والاستفادة منها في مختلف نواح الحياة تتمثل بالآتي (دشاش وصديقي، 115:2018):

أ. **عوامل تقنية**: إن الثورة الهائلة في عالم الاتصالات من خلال ما تتيحه شبكة الإنترنت أدى إلى إلغاء الحدود المكانية إذ أصبح العالم قرية واحدة وأصبح تدفق المعلومات من قارة إلى قارة يحدث في دقائق معدودة وكذلك تدفق المعلومات المحاسبية عِبرَ بيئات الأعمال مما اضطر الوحدات الاقتصادية إلى نشر تقاريرها الكترونياً عِبرَ مواقعها.

ب. **عوامل اقتصادية وسياسية**: إن ظهور التجارة الدولية غير الخريطة الاقتصادية والسياسية للعالم لأن ابرام الاتفاقيات ألزم هذه الدول على حرية دخول رؤوس الأموال والسلعة من دولة إلى أخرى مما أدت إلى إنشاء أسواق مالية لمواكبة التطورات التي مست التجارة الدولية فقد أصبح ملجأ لتدفق المعلومات بين هذه الدول والأسواق، وظهور ما يعرف بالتجارة الإلكترونية مما اضطر الوحدات الاقتصادية إلى الإفصاح الكترونياً عن تقاريرها المالية عبر مواقعها.

ج. **عوامل ثقافية واجتماعية**: إن التقارب الذي حصل بين الشعوب نتيجة لتحسين وتسريع وسائل النقل وكذلك تحسين وسائل الاتصال أدى إلى ظهور التسويق العالمي لِمُنتجات الوحدات الاقتصادية وكذلك سهولة الحركة بين هذه الدول أدى إلى سهولة حركة اليد العاملة مما جعل الحاجة مَلحة للحصول على

معلومات حول المنتجات العالمية وكذلك الحصول على معلومات بيئات الأعمال من أجل البحث عن فرص العمل، كل هذه العوامل أدت إلى ضرورة نشر الوحدات الاقتصادية تقاريرها المالية عِبرَ مواقعها الإلكترونية وجعلهُ أمراً الزامياً.

د. **عوامل محاسبية**: إن التطور في مجال المعلوماتية كان له أثر كبير في مجال المحاسبة، إذ إن مهنة المحاسبة كغيرها من المهن تأثرت بهذا التطور، فقد أصبح الزاماً على النظام المعلوماتي المحاسبي الاستعانة بالتقنيات الحديثة لمعالجة البيانات إذ تعالج كماً كبيراً من البيانات في وقت وجيز كما إن السرعة الفائقة في أداء العمليات الحسابية والمنطقية بدقة متناهية واجراء العديد من الاختبارات الرقابية المبرمجة مسبقاً والقدرة على تخزين كم هائل من البيانات بصور مختلفة كل ذلك أدى إلى الاستعانة بالحاسب من طرف نظام المعلومات المحاسبي مما أدى إلى ظهور المحاسبة الإلكترونية، ومع الكم الهائل الذي تنتجه هذه المحاسبة فضلاً الأشكال المختلفة لمخرجات هذه المحاسبة (PDF، EXCEL،WORD) وعليهِ لم يعد باستطاعة الإفصاح التقليدي عرض كل مخرجات المحاسبة الإلكترونية مما أصبح الزاماً الإفصاح عنها الكترونياً.

وهنا يتبن أنه يوجد العديد من العوامل التي كانت سببا في الحاجة إلى الإفصاح الإلكتروني، منها التطورات والابتكارات التكنلوجية المُستمرة والتشتت الجغرافي لأصحاب المصلحة في الوحدات، والأزمات السياسية والاقتصادية التي يمر بها البلاد تؤثر تأثيراً كبيراً على الوضع الاقتصادي بصورة عامة والبيئة الاستثمارية بصورة خاصة، وظهور التجارة الإلكترونية والحاجة إلى دخول رؤوس الأموال للبلاد عن طريق مستثمرين أجانب، فضلاً عن أن ظهور الانترنت وتوسعهُ حول العالم أدى إلى استخدامهِ في مجال بيئة الأعمال، وظهور المحاسبة الإلكترونية، كل هذه العوامل أدت إلى الحاجة إلى الإفصاح الإلكتروني.

المبحث الثاني: المخاطر السيبرانية

منذ بداية القرن الحالي شهد العالم زيادة ملحوظة في عدد وحجم الهجمات السيبرانية بحسب تقرير صادر عن مركز الدراسات الاستراتيجية والدولية، فأن التهديدات السيبرانية تكلف الاقتصاد العالمي مليارات الدولارات سنويًا.

وتؤثر المخاطر السيبرانية بشكل مباشر على السمعة والثقة المالية للشركات. فالهجمات الناجحة يمكن أن تؤدي إلى خسائر مالية كبيرة، وتوقف العمليات التجارية، وفقدان البيانات الحساسة للعملاء وهذا يجعل من الضروري للشركات أن تستثمر في الأنظمة الأمنية المتقدمة وتحديث سياساتها وإجراءاتها بشكل مستمر.

في ضوء ذلك لابد من بيان المقصود بها ووجهات نظر الكتاب والباحثين بصددها، إذ يمكن تعريف المخاطر السيبرانية على أنها خطر الخسارة المالية أو التعطيل أو الضرر الذي يلحق بسمعة الوحدة الاقتصادية من فشل أنظمة تكنولوجيا المعلومات الخاصة بها. هناك عدد من الأطر وطرق التقييم لتحديد خطر الإنترنت. ربما تم بالفعل اختيار واحد أو أكثر والموافقة عليه من قبل الوحدة الاقتصادية. إذا لم يكن الأمر كذلك، فمن المهم اختيار واحد والتصديق عليه لاستخدامه في تقييم المخاطر وعملية قياس الأداء. أن اختيار تقييم المخاطر على مستوى الوحدة الاقتصادية يسهل عملية قبول النتائج من قبل الهيئات الإدارية (Siegel & Sweeney, 2020: 96).

وعرفها (مطر، 2024: 8) بأنها مزيج من احتمالية وقوع حدث يهدد شبكة انظمة المعلومات وعواقب هذا الحدث على اصول وسمعه الوحدة الاقتصادية، وإن أحد أسباب المخاطر السيبرانية هي

ضعف البنية للشبكات المعلوماتية في الوحدات الاقتصادية وقابليتها للاختراق إذ إن شبكات المعلومات مصممة بشكل مفتوح دون حواجز امنية عليها ورغبة دخول المستخدمين ويمكن استغلال الثغرات الموجودة في الأنظمة والشبكات المعلوماتية بهدف التسلل إلى البنى المعلوماتية التحتية لأي وحدة اقتصادية وتخريبها (فرحات، 2019: 96).

وتتمثل الهجمات السيبرانية عدداً من المخاطر السيبرانية التي تضم بشكل خاص الآتي (الكرعاوي، 2024: 463):

1. **مخاطر سيبرانية تتعلق بالسرية**: إذ تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل الوحدة الاقتصادية إلى طرف ثالث كما في حالة حدوث اختراق البيانات.
2. **مخاطر سيبرانية تتعلق بالنزاهة**: التي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال.
3. **مخاطر سيبرانية تتعلق باستمرارية الأداء**: تتلخص في تعطل أو التوقف عن ممارسة الأعمال.

وهذه الأنواع الثلاثة من المخاطر السيبرانية لها تأثيرات مختلفة ومباشرة على الوحدات، إذ تؤدي لتعطل الأعمال وتحقيق خسارة وتعطل في تحقيق الأهداف، والتحقيق في تأثيرات اختراق البيانات قد يستغرق وقتاً طويلاً، وهذا ينتج عنه أضرار معنوية تمس السمعة فضلاً عن تكاليف التقاضي، وفي اعقاب الهجمات الإلكترونية قد يكون خطر فقدان الثقة عالياً بالنسبة للقطاع المالي وذلك، لاعتماد الوحدات الاقتصادية المالية على ثقة عملائها (البغدادي، 2021: 1464).

كما اتفقت دراستي (شحاته والبردان، 2021: 10) و(السواح، 2021: 511) على تصنيف المخاطر السيبرانية إلى ثلاثة أنواع من المخاطر على النحو الآتي:

- **المخاطر المتعلقة بتأمين البيانات والمعلومات**: وهي المخاطر الناشئة من تخرين البيانات والمعلومات للأفراد والوحدات الاقتصادية ومن الممكن تعرضها إلى الاختراق أو نقلها للمنافسين.
- **المخاطر المتعلقة بانتهاك الخصوصية:** وهي المخاطر الناتجة عن مخاطر سرقة البيانات الشخصية.
- **المخاطر المتعلقة بانتهاك حقوق الملكية الفكرية**: وتتمثل في المخاطر المتعلقة بحقوق الملكية الفكرية نتيجة نسخ الوسائط الرقمية وإعادة إنتاجها وتأخر مستوى التشريعات القانونية.

ووفقاً لما طرح من آراء يمكن أن توصف المخاطر السيبرانية بأنها تهديد أو تحدٍ يستهدف البيانات المخزنة أو المنقولة على الأنظمة الرقمية أو الشبكات أو الأجهزة الإلكترونية أو الإنترنت، وقد يؤدي إلى خسارة مالية أو تعطيل الخدمة أو انتهاك الخصوصية أو الإضرار بسمعة الوحدات وقد تؤدي إلى انهيارها. وفي ظل هذه البيئة المتسارعة والمليئة بالمخاطر يتطلب بالفعل ادراج الأمن السيبراني كحجر أساس في أي وحدة لضمان وضع استراتيجية محكمة ضد المخاطر السيبرانية واعتماد ضوابط وعمليات واضحة وقوية مبنية على اساسيات هامة للأمن السيبراني على مستوى الوحدة كلها إذ تحتاج هذه الوحدات إلى هياكل وعمليات فاعلة تمكنها من تحقيق أهدافها.

وباستقراء الفكر فيما يتعلق بتصنيف المخاطر السيبرانية التي تواجهها الوحدات الاقتصادية، لا تتعرض كل الصناعات بشكل متطابق للمخاطر السيبرانية. ويتوقف ذلك على عوامل عدة مثل طبيعة المخاطر وإمكانية حدوث خسائر، إذ تباينت الآراء حول التصنيفات المختلفة للمخاطر السيبرانية في القطاعات إذ يحكم التصنيف لأنواع المخاطر على الدافع إذ يمكن أن يكون البحث عن المكاسب المالية أو التنافسية، وتدمير البيانات، مسح البيانات السيبرانية أو تشفيرها أو منع الوصول إليها، او الدافع هو الابتزاز، وانقطاع الاتصالات، تعطيل الموقع الإلكتروني أو تعطيل الشبكة أو تشويه الموقع للاستيلاء على صفحات وسائل التواصل الاجتماعي والدافع هو الابتزاز أو التجسس.

وبسبب نمو تقنية الانترنت حصلت الجرائم السيبرانية على اهتمام كبير مقارنة بالجرائم التقليدية إذ يختلف مفهوم الجريمة السيبرانية اختلافاً كبيراً عن المفهوم التقليدي للجريمة وذلك بسبب وجود العديد من الخصائص المميزة للجرائم السيبرانية ومن أهم هذه الخصائص (سالم، 2023: 981):

1. **الاشخاص ذوي المعرفة المتخصصة:** الجرائم السيبرانية هي جرائم يمكن ارتكابها فقط من خلال التقنية لذا من اجل ارتكاب هذا النوع من الجرائم يجب أن يكون لدى الشخص مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسوب والإنترنت.
2. **الامتداد العالمي:** في الفضاء السيبراني لا يوجد حدود، وان الجريمة السيبرانية هي جريمة ذات بعد دولي، أي أنها عابرة للحدود وهذا يعني أن مرتكبي جرائم الأمن السيبراني لديهم القدرة على ارتكاب الجرائم عن بعد والتأثير على الضحايا في أي مكان في العالم، ويعد هذا أحد الخصائص الرئيسة لجرائم الأمن السيبراني مما يجعلها تختلف عن جميع أنواع الجرائم التقليدية وأيضاً يجعلها معقدة للغاية.
3. **صعوبة جمع الادلة:** جزء اساس من الإفصاح عن الجرائم هو جمع ومعالجة الادلة الرقمية ولكن من الصعب للغاية جمع الأدلة فيما يتعلق بالجرائم السيبرانية ويرجع ذلك إلى أسباب عديدة على سبيل المثال طبيعة بيانات الكمبيوتر نفسها إذ تعد سريعة الزوال كذلك الامتداد الدولي للجرائم السيبرانية واختلاف القوانين بين الدول ومن ثم هناك صعوبة في التحقق فيها وكذلك اثباتها أمام القضاء نظرا لطبيعتها.
4. **حجم آثار جرائم الأمن السيبراني لا يمكن تصوره:** تعد جرائم الأمن السيبراني أكبر تهديد يواجه الوحدات الاقتصادية في الوقت الحالي وواحدة من أكبر التحديات التي ستواجه البشرية وذلك على المدى العقدين المقبلين وبالنسبة للمنشآت فأن التكاليف والخسائر المرتبطة بالجرائم السيبرانية ضخمة إلى حد لا يمكن تخيله فقد تسبب تلف البيانات أو سرقتها، سرقة الأموال، الملكية الفكرية، البيانات الشخصية والمالية، تعطيل أعمال الوحدة بعد تعرضها لهجوم سيبراني كالأضرار بسمعة الوحدة وفقدان الانتاجية وتغير ارقام البيانات في السجلات المخزنة في ذاكرة الحاسبات وغير ذلك من الآثار ويمكن أن تسبب الجرائم السيبرانية في كل ذلك دون أن يكون لها أي أثر خارجي مرئي.

مما سبق يتضح أن المخاطر السيبرانية تُشكّل تحديًا كبيرًا يهدد الأفراد والوحدات الاقتصادية على حد سواء وهو يعكس مدى التعقيد الذي ينطوي عليه الأمن السيبراني في العصر الحديث، كما يتضح أن تصنيف المخاطر السيبرانية يتركز في الدوافع المختلفة مثل المكاسب المالية، التجسس، أو الإرهاب مما يعكس تنوع الهجمات السيبرانية واختلاف طبيعتها بناءً على الأهداف.

وتتعدد مصادر المخاطر السيبرانية التي تهدد استقرار وأمن الوحدات الاقتصادية، ويمكن تصنيفها إلى أربعة محاور رئيسة وهي متداخلة وتؤثر بشكل مباشر على فعالية أنظمة المعلومات وأمنها وهذه المصادر هي:

1. **المصادر البشرية**: تُعد الأخطاء البشرية وسوء السلوك من أبرز العوامل المسببة للهجمات السيبرانية، سواء كانت ناتجة عن الجهل أو الإهمال أو النية الخبيثة، فوفقًا لتقرير Verizon Data Breach Investigations Report هو تقرير سنوي تصدره شركة Verizon الأمريكية وهي واحدة من أكبر شركات الاتصالات في العالم إذ يُعد تقريرها من أهم المصادر الموثوقة في تحليل أنماط اختراق البيانات والانتهاكات الأمنية التي تتعرض لها الوحدات الاقتصادية في مختلف القطاعات فإن 82% من الخروقات الأمنية تعود إلى العامل البشري، سواء عبر رسائل التصيّد الاحتيالي أو استخدام

كلمات مرور ضعيفة، كما إن غياب التوعية أو ضعف ثقافة الأمن الرقمي يُفاقم هذه المخاطر (Verizon, 2022: 7).

2. **المصادر التقنية**: تتمثل في الثغرات البرمجية، وضعف التحديثات الأمنية، وسوء تكوين الشبكات، مما يُتيح للمهاجمين استغلال تلك الفجوات، وتشير دراسة (Grimes, 2019: 153) إلى أن عدم تصحيح الثغرات هو أحد أهم مسببات الهجمات على الأنظمة، إلى جانب استخدام أنظمة قديمة غير مدعومة.
3. **المصادر التنظيمية والإدارية**: غالباً ما تنشأ المخاطر السيبرانية نتيجة لغياب السياسات الأمنية الواضحة أو عدم تطبيقها بصرامة، ووفقًا لتقرير صادر عن ISACA فإن العديد من الوحدات الاقتصادية تفشل في تطبيق إطار حوكمة فعال للأمن السيبراني، مما يؤدي إلى ضعف في الرقابة الداخلية وسهولة استهدافها (ISACA, 2015: 23)
4. **المصادر الخارجية**: تشمل هذه الفئة الجهات الخارجية التي تستهدف الأنظمة، مثل المخترقين، ومجموعات الجريمة المنظمة، وأطراف دولية معادية، وإن الهجمات التي تُشن من خارج الوحدة الاقتصادية باتت أكثر تعقيدًا وتعتمد على أدوات متطورة يصعب اكتشافها بسرعة (IBM, 2023: 12)

وتُشكّل المخاطر السيبرانية تهديدًا متصاعدًا على الوحدات الاقتصادية في ظل الاعتماد الواسع على نظم المعلومات الرقمية، مما يجعل هذه الوحدات عرضة لآثار متعددة تمسُّ الجوانب المالية والتشغيأتية والسمعية والقانونية .وتُظهر الدراسات أن الهجمات السيبرانية لا تؤدي فقط إلى خسائر مادية مباشرة، بل تتسبب أيضًا في اضطرابات مستمرة قد تُقوّض استمرارية الأعمال وتهدد بقاء الكيان الاقتصادي، ومن أبرز هذه الآثار ما يأتي:

1. **الآثار المالية المباشرة:** تتمثل في خسائر فورية ناجمة عن سرقة الأموال، أو دفع فديات كما في حالات هجمات، أو تكاليف استعادة البيانات والأنظمة. ووفقًا لتقرير IBM (2023)، إذ بلغ متوسط تكلفة اختراق البيانات عالميًا حوالي 4.45مليون دولار للوحدة الاقتصادية الواحدة (IBM, 2023: 8).
2. **انقطاع العمليات التشغيأتية**: تؤدي الهجمات السيبرانية إلى توقف الأنظمة الحيوية داخل الوحدة الاقتصادية، مما يُعطّل سلسلة التوريد، والمعاملات التجارية، ويؤثر على كفاءة الأداء التشغيأتي، وهو ما يُهدد بعجز قصير أو طويل الأجل في تلبية الطلبات.
3. **الإضرار بالسمعة والثقة**: غالبًا ما تؤدي الحوادث السيبرانية إلى فقدان ثقة الزبائن والمستثمرين، خصوصًا في حالات تسريب البيانات الشخصية أو المالية الحساسة، مما يؤثر على القيمة السوقية للوحدة الاقتصادية (ENISA, 2022: 17)
4. **التعرض للمساءلة القانونية والتنظيمية**: في حال عدم التزام الوحدة الاقتصادية بالضوابط التنظيمية المتعلقة بحماية البيانات (مثل قوانين الخصوصية المحلية)، فإنها قد تتعرض لغرامات قانونية وعقوبات صارمة، وقد تصل إلى نسب مئوية من الايرادات السنوية.
5. **زيادة التكاليف التأمينية والتدقيقية**: تؤدي المخاطر السيبرانية إلى ارتفاع في أقساط التأمين على أمن المعلومات، كما تتطلب الوحدة الاقتصادية تخصيص موارد أكبر للتدقيق والتقييم الأمني الدوري (PwC, 2022, 11).
6. **فقدان البيانات**: تتسبب بعض الهجمات في تسريب أو تدمير بيانات ذات طابع استراتيجي أو بحثي، مما يؤدي إلى خسارة ميزة تنافسية أو اختلال في قرارات التخطيط طويلة الأمد.

7. **ضعف الامتثال والمراجعة الداخلية**: تشير بعض الدراسات إلى أن المخاطر السيبرانية تكشف ثغرات في الرقابة الداخلية ونظم الحوكمة، ما يدفع الوحدات الاقتصادية إلى مراجعة سياساتها الأمنية وتحديث بنيتها التحتية التكنولوجية بشكل عاجل (ISACA, 2021: 19)

ويرى الباحثان أن المخاطر السيبرانية لم تعد مجرد تهديدات تقنية محصورة في نطاق نظم المعلومات، بل أصبحت تمثل أحد أبرز محددات الاستقرار المالي والتشغيأتي للوحدات الاقتصادية، لاسيما مع توسّع الاعتماد على البيئة الرقمية. كما إن آثار هذه المخاطر تتجاوز الخسائر المباشرة لتُهدد بفقدان الثقة المؤسسية والإضرار بالحوكمة الداخلية، مما يستلزم من الوحدات الاقتصادية تعزيز استثماراتها في الأمن السيبراني ليس فقط كإجراء دفاعي، بل كجزء من استراتيجية إدارة المخاطر الشاملة، لضمان الاستدامة وتعزيز التنافسية في ظل بيئة أعمال تتسم بالتغير السريع والتهديدات المتطورة.

المبحث الثالث: متطلبات الإفصاح عن المخاطر السيبرانية

يمكن للوحدات الاقتصادية الحد من حالة عدم اليقين، وجعل الاستثمار في أسهمها أكثر جاذبية، من خلال توفير افصاحات إضافية عن إدارة المخاطر (Deumes & chel, 2008,: 35). إذ أن الهجمات الإلكترونية مكلفة في الكثير من الأحيان، وتؤثر سلباً على الأداء المالي للوحدة الاقتصادية، ويعدها المستثمرين من أهم المخاطر التي تهدد نمو وبقاء الوحدة الاقتصادية.

لذا بدأت المنظمات المهنية تولي اهتماماً متزأيداً بالإفصاح عن مخاطر الأمن السيبراني منذ عام 2011 كما طور المعهد الأمريكي للمحاسبين القانونيين (AICPA) إطار عمل اختياري بالتعاون مع مجلس معايير المراجعة Auditing Standards Board يهدف هذا الإطار إلى وضع أسس لإعداد تقارير إدارة مخاطر الأمن السيبراني (AICPA, 2017: 3). ويوفر هذا الإطار المفاهيمي وصفاً سردياً لبرنامج إدارة مخاطر الأمن السيبراني للوحدة الاقتصادية، والتأكيدات فيما يتعلق بما إذا كان هذا الوصف يتوافق مع إرشادات المعهد الأمريكي للمحاسبين القانونيين، وما إذا كانت الضوابط الموضوعة ضمن برنامج إدارة مخاطر الأمن السيبراني فعّالة خلال الفترة المشمولة بالتقرير.

كما يهدف هذا الإطار إلى توفير لغة مشتركة يمكن لأصحاب المصالح استخدامها لتقييم موقف الأمن السيبراني للوحدة وفعالية برنامج إدارة المخاطر الخاص بها (Yang et al., 2020: 4) في ضوء ما تقدم، يُلاحظ أن مخاطر الأمن السيبراني أصبحت من المعلومات الضرورية لترشيد قرارات المستثمرين. كذلك فإن تنظيم هذا الإفصاح سوف يساهم في ترشيد القرارات الاستثمارية، وفي الوقت نفسه سوف يُحسن أداء الوحدة الاقتصادية في مجال إدارة مخاطر الأمن السيبراني، حتى تتجنب الإفصاح عن أية معلومات سلبية في هذا المجال.

وأصبح الإفصاح عن المخاطر السيبرانية من الممارسات الجوهرية في بيئة الأعمال الرقمية، خصوصًا في ظل تصاعد التهديدات الإلكترونية التي قد تؤثر على استدامة الوحدات الاقتصادية وسلامة معلوماتها وسمعتها المالية. إذ لم يعد الإفصاح محصورًا في الجوانب التقليدية للمخاطر المالية، بل توسع ليشمل المخاطر غير المالية، وعلى رأسها المخاطر السيبرانية، التي باتت تؤثر بعمق في قرارات المستثمرين وفعالية الحوكمة المؤسسية (COSO, 2020: 9).

ويُشير الإفصاح السيبراني إلى عملية تقديم معلومات مفصلة وموثوقة لأصحاب المصلحة حول طبيعة التهديدات الإلكترونية التي قد تواجهها الوحدة الاقتصادية، ومدى تأثيرها المحتمل على

أنظمتها وعملياتها، فضلاً عن السياسات والإجراءات الأمنية المتبعة لإدارتها. ووفقًا لإرشادات هيئة الأوراق المالية والبورصات الأمريكية (SEC)، فإن على الوحدات الاقتصادية الإفصاح عن أي مخاطر سيبرانية جوهرية قد تؤثر على نتائجها المالية أو استمراريتها، سواء وقعت تلك الأحداث أم أنها محتملة الوقوع (SEC, 2018: 4)

وتتضمن عناصر الإفصاح عن المخاطر السيبرانية عادةً ما يأتي:

1. توصيف الهجمات أو التهديدات التي تعرضت لها الوحدة الاقتصادية أو القطاعات المماثلة.
2. تقييم أثر تلك التهديدات على الأداء المالي والتشغيلي.
3. الإجراءات التصحيحية أو الوقائية المُتبعة (مثل أنظمة الحماية، خطط الاستجابة).
4. سياسات الامتثال للأطر القانونية والتنظيمية ذات العلاقة.

ويُعد الإفصاح الشفاف والمتكامل عن هذه المخاطر أداة أساسية لتحقيق الثقة المؤسسية، إذ يُمكّن لأصحاب المصلحة من تقييم مدى قدرة الإدارة على رصد المخاطر والتصدي لها، كما يسهم في خفض فجوات المعلومات التي قد تؤدي إلى تضليل المستثمرين أو تعريض الوحدة الاقتصادية لمسؤوليات قانونية.

وقد بيّنت دراسات مهنية مثل تقرير (PwC, 2023: 21) أن الوحدات الاقتصادية التي تُفصح بوضوح عن مخاطرها السيبرانية تحظى بتقييم أعلى من حيث الجدارة الائتمانية والثقة الاستثمارية، مقارنة بالوحدات الاقتصادية التي تتجاهل هذه المخاطر أو تقلل من الإفصاح بشأنها.

الإفصاح عبر الإنترنت ووسائل التواصل الاجتماعي أدى إلى التحسين في بيئة المعلومات من خلال أبعاد عدة، لعل أهمها ما يأتي (Hamm, 2019, 10): (تحسين الوصول إلى المعلومات، تخفيض تماثل المعلومات وتحسين سيولة السوق، تخفيض مخاطر المعلومات وزيادة جودة ومستوى الإفصاح والشفافية، تخفيف رد فعل السوق السلبي).

ويعد الإفصاح المحاسبي الإلكتروني عن المخاطر السيبرانية من المجالات البحثية التي نالت حيزاً واسعاً في المجال المحاسبي. إذ يضع المحاسبون حوادث الأمن السيبراني أخذين في الاعتبار المخاطر السيبرانية أثناء تقييم المخاطر.

والإفصاح الإلكتروني عن المخاطر السيبرانية هو الإفصاح العام عن المعلومات المتعلقة بحادث أمن البيانات، ويسمح للشركات بإيصال المعلومات البارزة إلى الأطراف المعنية وأصحاب المصلحة فيما يتعلق بطبيعة وتأثير الخرق (Kelton & Pennington, 2020: 139).

والإفصاح الإلكتروني عن المخاطر السيبرانية؛ هو عملية من الإجراءات والضوابط المنطقية التي تمارسها المنظمات للإفصاح عن المعلومات المحيطة بالخرق الأمني، من خلال التأثيرات المختلفة لأصحاب المصلحة، والعوامل الداخلية والخارجية، وغالباً ما تؤدي العملية إلى درجات متفاوتة من الاكتمال والدقة وحسن التوقيت والشفافية ومشاركة الإدارة في المعلومات لاتخاذ القرارات، واعطاء الفرصة لاستكشاف وفهم الظاهرة والتحقيق في القضايا ذات الصلة.

وتكمن أهمية الإفصاح الإلكتروني عن المخاطر السيبرانية في إظهار جميع المعلومات الضرورية وتلبية احتياجات مستخدمي التقارير المالية عبر موقع الوحدة الاقتصادية وغيرها من التقارير لمساعدتهم في اتخاذ القرارات، وتخفيض حالة عدم التأكد (يوسف، 2022: 48).

إن الارتباط الإيجابي بين الإفصاح الإلكتروني عن الأمن السيبراني وجاذبية الاستثمار يعتمد على الإفصاح عن مسؤولية الإدارة العليا، أن الوحدات الاقتصادية بحاجة إلى الإفصاح عن

المخاطر السيبرانية التي واجهتها، والمحتملة لتعزيز الإفصاح والشفافية في تقاريرها السنوية (يعقوب وآخرون، 2022: 1409).

ويرى الباحثان أن الإفصاح الإلكتروني عن المخاطر السيبرانية هو القدرة على توفير المعلومات لوصف المخاطر السيبرانية، والاستجابة لها وتخفيفها في التقرير السنوي، وبيان أثارها الاقتصادية المتوقعة على الأداء الحالي والمستقبلي، لتقليل درجة عدم التأكد الذي يحيط بالخدمات الرقمية في الفضاء السيبراني.

وإن النظرة المتعارف عليها تركز على تقليل عدم تناسق المعلومات بين المديرين وأصحاب المصلحة، إذ يجب على الوحدات الاقتصادية تزويد مستثمريها والسوق بمعلومات فورية بشأن أي مخاطر حقيقية تؤثر على أعمالهم، من أجل الحفاظ على برنامج فعال لإدارة المخاطر، ويجب الاعتماد على خمسة مراحل تتمثل بالآتي:

- ❖ تحديد مخاطر التعرض للأمن السيبراني وتحديد أولوياتها.
- ❖ تصميم نظام مراقبة الأمن السيبراني.
- ❖ اختبار الفعالية التشغيأتية لضوابط الأمن السيبراني.
- ❖ إعداد التقارير الخارجية عن الأمن السيبراني.
- ❖ توفير ضمانات بشأن التقارير الخارجية عن الأمن السيبراني.

إذ يمكن لشركات المحاسبة تقديم ضماناً رسمياً مهنياً ومستقلاً بشأن فعالية برنامج إدارة المخاطر السيبرانية، وتتمثل المتطلبات الأساسية للإفصاح عن المخاطر السيبرانية فيما يأتي (موسى، 2023: 19):

1. **الإفصاح عن عامل التهديد وطبيعة التهديد ومواطن الضعف**: يستخدم مصطلح عامل التهديد أو ممثل التهديد للإشارة إلى فرد أو مجموعة يمكن أن تظهر تهديداً لسرية موارد النظام وسلامتها وتوافرها، ويمكن لعامل التهديد اتخاذ واحد أو أكثر من الإجراءات الآتية ضد أحد الأصول: الوصول غير المصرح به والاستخدام غير المصرح به للأصول والإفصاح عن عامل التهديد بشكل غير قانوني عن معلومات حساسة، والتعديلات أو التغييرات غير المصرح بها على أحد الأصول، ورفض الوصول بما في ذلك التدمير، ومنع الوصول المصرح به، ومن المهم إدراك أن كل إجراء من هذه الإجراءات يؤثر على الأصول، وتؤثر الإجراءات على الأصول إلى اختلاف طبيعة التهديد، على سبيل المثال، تعتمد احتمالية خسارة الإنتاجية الناتجة عن الأصول المدمرة أو المسروقة على مدى أهمية هذا الأصل في إنتاجية الوحدة الاقتصادية وطبيعة الأصل، ويمكن للأصول المتعلقة بالمخاطر السيبرانية أن تمثل نقاط ضعف، وتتجسد المخاطر السيبرانية في استغلال نقاط الضعف هذه (Luque et al., 2021: 187). وربطت الأبحاث المحاسبية السابقة بين حوادث الأمن السيبراني ونقاط الضعف المحتملة في الرقابة الداخلية وأوجه القصور في التقارير المالية، وهذا الربط يستلزم تضمين إجراءات مراجعة موضوعية لضوابط الأمن السيبراني لضمان مراجعة اختبارات تصميم وفعالية التحكم السيبراني بدقة لتوفير ضمان الأداء السليم لنظام الرقابة الداخلية داخل الوحدة الاقتصادية.

إن نقاط الضعف والثغرات الأمنية التي لم يتم إصلاحها يمكن أن تتسبب في مشكلات خطيرة، وعلى سبيل المثال قد يكون للثغرة الأمنية غير المعالجة في نظام تشغيل واسع الاستخدام عواقب سلبية وخيمة إذ يمكن أن تؤثر على ملايين المستخدمين والوحدات الاقتصادية.

2. **الإفصاح عن عمليات الاكتشاف والتحقق:** الاكتشاف هو عملية رصد ومراقبة الأحداث التي تحدث في نظام كمبيوتر أو شبكة وتحليلها بحثاً عن علامات لحوادث محتملة، والتي تمثل انتهاكات أو تهديدات وشيكة بانتهاك سياسات أمان الكمبيوتر أو سياسات الاستخدام المقبولة، ويجب أن تتكون ضوابط الإفصاح في بيئة رقابة سليمة وكافية، والغرض من الإفصاح عند الاكتشاف هو أن يتم إبلاغ توقيت الاقتحام وتوقيت الاكتشاف إلى الأطراف المعنية ذات الصلة، ويمكن أن يكون الفاصل الزمني بين وقت الحادث ووقت الاكتشاف مؤشراً مهماً لمدى جودة عمل ضوابط الاكتشاف، وبدون هذا الإفصاح لن يتمكن الإفصاح عن الانتهاكات من إبلاغ أصحاب المصلحة المعنيين بالمحتوى التالي من المعلومات (توقيت ووسيلة وطريقة الاقتحام، وما هو الوقت الذي تستغرقه الوحدة للرد؟ ما هي الإجراءات التي يتم اتخاذها فور اكتشاف الاقتحام؟، وما هي الأطراف المشاركة في عملية الاكتشاف والتحقيق؟).
3. **الإفصاح عن تقييم المخاطر وتحليل الأثر:** يتيح الإفصاح عن تقييم المخاطر وتحليل الأثر لأصحاب المصلحة بالتعرف على الآثار المحتملة للخسارة، وتتيح المعلومات الواردة في تقييم المخاطر وتحليل الأثر لصانعي القرار بتقييم مدى أهمية الحدث وتحديد أولويات التعامل مع الحادث، وإنه يجب تقييم تأثير الخرق الأمني وفقاً لما يأتي: (الأثر الوظيفي للحادث، وتأثير الحادث على المعلومات، والقدرة على التعافي من الحادث) وأوصى المعهد الأمريكي للمحاسبين القانونيين (AICPA, 2017) لمراقبة الأمن السيبراني لتحقيق أهدافه بما يأتي (Grove & Schaffiner, 2019: 93):

- ❖ يستخدم الكيان إجراءات الإفصاح والمراقبة لتحديد التغييرات على التكوينات التي تؤدي إلى إدخال ثغرات أمنية جديدة.
- ❖ يقوم الكيان بمراقبة مكونات النظام، وتشغيل تلك المكونات للكشف عن الحالات الشاذة التي تدل على الأفعال الكيدية والكوارث الطبيعية والأخطاء، والتي تؤثر على قدرة الكيان على تحقيق أهدافه، ويتم تحليل الحالات الشاذة لتحديد ما إذا كانت تمثل أحداثاً أمنية.
- ❖ يقوم الكيان بتقييم الأحداث الأمنية لتحديد ما إذا كان من الممكن تجنب الحوادث الأمنية، وإذا كان الأمر كذلك، تتخذ إجراءات لمنع أو معالجة مثل هذه الإخفاقات.
- ❖ يستجيب الكيان للحوادث الأمنية التي حددت عبر تنفيذ برنامج استجابة محدد للحوادث، لفهم الحوادث الأمنية واحتوائها ومعالجتها والإبلاغ عنها.
- ❖ يقوم الكيان بتحديد وتطوير وتنفيذ أنشطة التعافي من الحوادث الأمنية التي حددت.
- ❖ ووفقاً لإرشادات لجنة الأوراق المالية والبورصات الأمريكية (SEC) لعام (2018) أنه عند مراجعة قواعد الإفصاح الإلكتروني عن قضايا الأمن السيبراني يجب مراعاة ما يأتي:

أ. **الأهمية النسبية**: ينبغي التركيز على توجيه الاهتمام نحو المخاطر السيبرانية عند إعداد تقارير الإدارة السنوية، ولاسيما الحوادث الهامة من وجهة نظر المستثمرين والأضرار الناتجة عنها. وتعتمد الأهمية النسبية للمخاطر السيبرانية على مدى الضرر الذي يمكن أن تسببه مثل هذه الحوادث، وهذا يشمل الضرر الذي يلحق بسمعة الوحدة الاقتصادية، والأداء المالي، والعلاقات مع الزبائن، وإمكانية التقاضي أو الإجراءات التنظيمية.

ب. **وصف عوامل الخطر السيبراني وطبيعة الأنشطة**: يجب الإفصاح عن الحوادث السيبرانية الفعلية والمتوقعة والتي تمثل مخاطر خاصة على الوحدة الاقتصادية في سياق الإفصاح عن إدارة المخاطر

السيبرانية، ويجب الإفصاح عن أي حوادث سيبرانية يكون لها تأثير جوهري على طبيعة نشاط الوحدة الاقتصادية والعلاقات مع الموردين أو الزبائن، ويجب الإفصاح عن أي قضايا متعلقة بإدارتها.

ج. **سياسات الإفصاح في القوائم المالية ونتائج الأعمال**: يجب الإفصاح عن المخاطر السيبرانية التي لها تأثير جوهري على المركز المالي ونتائج الأعمال، وقد تؤثر المخاطر السيبرانية على عناصر القوائم المالية من ايرادات أو مصروفات أو تدفقات نقدية، وبالتالي لابد من الإفصاح عن هذه الأثار ضمن الايضاحات المتممة للقوائم المالية.

وأوضحت دراسة (الرشيدي وعباس، 2019، 461) بأن الإفصاح في التقارير المالية يتأثر بالمخاطر السيبرانية التي تواجهها الوحدة الاقتصادية؛ إذ يمكن أن تؤدي إلى: (زيادة المصروفات المتعلقة بالتحقيق والاخطار بالاختراق وكيفية علاجها، وانخفاض الايرادات إذ يتعين إما تقديم مزيد من الحوافز للعملاء للحفاظ عليهم وإلا يتم خسارتهم، والمطالبات المتعلقة بالضمانات وعدم الوفاء بالعقد واسترجاع المنتج والتعويضات للأطراف، وانخفاض التدفقات النقدية المستقبلية أو اضمحلال الأصول الفكرية أو غير الملموسة، وغيرها من الأصول فضلاً عن الاعتراف بمزيد من الالتزامات وزيادة تكاليف التمويل).

د. **دور مجلس الإدارة**: الإفصاح عن دور مجلس الإدارة بخصوص برنامج إدارة المخاطر السيبرانية، الذي يؤثر أيجاباً على المستثمرين، وعلى الرغم من عدم وجود تنظيم حصري للإفصاح عن معلومات الأمن السيبراني في التقرير السنوي.

4. **الإفصاح عن العلاج والاحتواء والرقابة التصحيحية والوقائية**: إن الاحتواء والضوابط التصحيحية هي عناصر مهمة في الإفصاح، ويشير إلى أن الوحدة الاقتصادية على رأس الانتهاك وقادرة على احتواء ومنع الحوادث المستقبلية، ويمكن أن يشمل الإفصاح عن ضوابط الاحتواء والرقابة التصحيحية والوقائية، ما يأتي: إجراءات لمنع الضرر المحتمل للموارد وسرقتها، وإجراءات للحفاظ على توافر الخدمات مثل الربط الشبكي والخدمات المقدمة إلى أطراف خارجية)، وفعالية الاستراتيجية مثل (الاحتواء الجزئي والكامل)، ومدة الحل على سبيل المثال حل الطوارئ المراد إزالته في غضون أربع ساعات، والحل المؤقت الذي يتعين إزالته في غضون أسبوعين والحل الدائم. وأوصى معهد المحاسبين القانونيين (AICPA) لمراقبة الأمن السيبراني وتخفيف المخاطر بأن يقوم الكيان بتحديد وتطوير أنشطة التخفيف من المخاطر الناشئة عن الاضطرابات التجارية المحتملة وأن يقوم الكيان بتقييم وإدارة المخاطر السيبرانية، ويجب أن تضمن إجراءات الإفصاح أن المعلومات المتعلقة بالمخاطر السيبرانية تتم معالجتها والإفصاح عنها.

ويرى الباحثان أنه من الضروري التحقق من جودة الإفصاح الإلكتروني عن المخاطر السيبرانية، وأن يتضمن الإفصاح الإلكتروني معلومات ذات قيمة لمتلقيها لمساعدة أصحاب المصلحة على اتخاذ القرارات بعد حدوث الخرق الأمني، وتتعلق بوصف مصادر التهديد والغرض منه، وطبيعة الأحداث والآثار المحتملة والحل المحتمل، ويجب أن تكون لدى الوحدات الاقتصادية سياسات وضوابط أمنية كافية، لتمكين الإفصاح الداخلي عن المشاكل الأمنية بحيث يتم إبلاغ الإدارة العليا ومجلس الإدارة بشفافية، وأن تسعى الإدارة العليا إلى الإشارة لمسؤوليتها تجاه أصحاب المصلحة، وذلك لتحقيق مجالات جودة الإفصاح عن المخاطر السيبرانية.

المحور الرابع: الاستنتاجات والتوصيات

أولاً. الاستنتاجات:

1. هناك تفاوت ملحوظ بين الشركات في الإفصاح عن التهديدات السيبرانية، سواء من حيث مستوى التفصيل، أو تحديد الأثر المالي المتوقع، أو الاستراتيجيات المتبعة للوقاية والمعالجة، مما يُضعف قابلية المقارنة بين التقارير ويؤثر على جودة اتخاذ القرار من قبل المستخدمين.
2. لا يزال الإفصاح عن المخاطر السيبرانية يعاني من ضعف في الشمولية وغياب الاتساق، فضلاً عن عدم وجود إطار إلزامي موحد، مما يقلل من فاعليته في مساعدة أصحاب المصلحة على اتخاذ قرارات مبنية على معلومات كافية.
3. إن الإفصاح عن المخاطر السيبرانية لا يتم وفق إطار منظم وموحد، وغالبًا ما يرد بشكل محدود أو غير مباشر ضمن تقارير الإدارة أو الحوكمة، مما يعكس غياب الوعي المؤسسي الكافي بأهمية هذه المخاطر ضمن منظومة الإفصاح الشامل.

ثانياً. التوصيات:

1. ضرورة تطوير إطار تنظيمي واضح وملزم للإفصاح عن المخاطر السيبرانية، بما يتوافق مع المعايير الدولية مثل COSO و NISTوISO 27001، ويُدمج ضمن معايير الإفصاح المالي والحوكمة لتعزيز الشفافية والثقة في التقارير المالية.
2. ضرورة تنظيم ورش عمل وبرامج تدريبية متخصصة للعاملين في أقسام المحاسبة وإعداد التقارير في الشركات حول كيفية رصد وقياس والإفصاح عن الحوادث السيبرانية، بالتعاون مع خبراء تكنولوجيا المعلومات والمخاطر.
3. إصدار تعليمات واضحة ومُلزمة للشركات بشأن الإفصاح عن الحوادث السيبرانية، مع تحديد نوعية المعلومات المطلوب الإفصاح عنها، وتوقيتها، ومكان ظهورها في التقارير المالية أو الحوكمة.

المصادر

اولاً. المصادر الأجنبية:

1. البغدادي، السيد أحمد عبد المقصود، 2021، الحوكمة الرقمية والأمن السيبراني: إطار متكامل لإدارة المخاطر في الوحدات الاقتصادية الحكومية، المركز القومي للبحوث الاجتماعية والجنائية، مصر.
2. بيومي، أحمد عبد الله، 2018، دور المراجعة الإلكترونية في تحسين كفاءة إدارة المخاطر في بيئة الأعمال الذكية، مجلة البحوث المالية والتجارية، جامعة الأزهر، العدد 2.
3. دشاش، إبراهيم، صديقي، نوال. 2018، حوكمة تكنولوجيا المعلومات ودورها في تعزيز فعالية نظام الرقابة الداخلية في ظل المخاطر السيبرانية، مجلة البحوث الاقتصادية المتقدمة، المجلد 5، العدد 1.
4. رشيد، عبد الله عبد الكريم. 2011، الإفصاح المحاسبي عن المخاطر وأثره في دعم قرارات مستخدمي القوائم المالية: دراسة تحليلأتية تطبيقية، المجلة العراقية للعلوم الإدارية، المجلد 7، العدد 27.
5. الرشيدي، طلال عبد الله، وعباس، عبد الرضا عباس. 2019، دور الإفصاح عن المخاطر السيبرانية في تعزيز مصداقية القوائم المالية: دراسة تطبيقية في بيئة الأعمال العراقية، مجلة الدراسات المحاسبية والمالية، جامعة الكوفة، المجلد 14، العدد 4.
6. سالم، عبد الحكيم محمود. 2023، تأثير المخاطر السيبرانية على ممارسات التدقيق المالي في بيئة الأعمال الرقمية، المجلة العراقية للعلوم المحاسبية والمالية، المجلد 18، العدد 3.

7. سليمان، محمد عبد القادر. 2018، تأثير تبني أدوات تكنولوجيا المعلومات في تطوير نظم الرقابة الداخلية على المخاطر الإلكترونية، المجلة الأردنية في إدارة الأعمال، المجلد 14، العدد 1.
8. السواح، حسام عبد الله. 2021، دور التدقيق الداخلي في إدارة مخاطر الأمن السيبراني: دراسة تحليأتية تطبيقية، مجلة البحوث المحاسبية، جامعة الإسكندرية، المجلد 22، العدد 4.
9. شحاته، أحمد عبد المنعم، البردان، حسين، 2021، أثر تطبيق معأيير الإفصاح عن المخاطر على جودة التقارير المالية في ظل التهديدات السيبرانية، مجلة البحوث المالية والتجارية، جامعة الأزهر، العدد 2، مصر.
10. الشطناوي، محمد عبد الكريم. 2018، أثر استخدام نظم المعلومات المحاسبية المحوسبة في تحسين جودة الرقابة الداخلية في ظل بيئة الأعمال الإلكترونية: دراسة ميدانية على البنوك الأردنية، المجلة الأردنية في إدارة الأعمال، المجلد 14، العدد 2.
11. عبار، زينب عبد الله. 2022، تأثير تبني إطار COBIT في تحسين استجابة التدقيق للمخاطر السيبرانية: دراسة تطبيقية في البيئة المصرفية العراقية، الجامعة المستنصرية، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة.
12. فرحات، عبد الرزاق. 2019، الأمن السيبراني ودوره في حمأية المعلومات في البيئة الرقمية، دار صفاء للنشر والتوزيع، الأردن.
13. القزاز، مازن أحمد، السقا، زياد هاشم، 2019، أثر ممارسات الحوكمة في تقليل مخاطر الأمن السيبراني: دراسة تحليأتية في البيئة الجامعية العراقية، مجلة تنمية الرافدين، المجلد 41، العدد 3.
14. الكرعاوي، أحمد جاسم محمد. 2024، الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ضوء المعأيير الدولية للتقارير المالية: دراسة تطبيقية، جامعة الكوفة، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة، العراق.
15. محسن، محمد عبد اللطيف، وآخرون. 2017، تأثير الإفصاح عن المخاطر غير المالية على جودة التقارير المالية في ظل المعأيير الدولية، مجلة المحاسبة والمراجعة، كلية التجارة، جامعة القاهرة، العدد 45.
16. مطر، نزار. 2024، التدقيق السيبراني كمدخل لتعزيز فعالية أنظمة الرقابة الداخلية في الوحدات الاقتصادية، دار الكتاب الأكاديمي، لبنان.
17. موسى، سنان جبار. 2023، أثر تطبيق الحوكمة السيبرانية في تعزيز جودة التقارير المالية: دراسة تحليأتية في عينة من الشركات المدرجة في سوق العراق للأوراق المالية، مجلة المحاسب العراقي، المجلد 24، العدد 2.
18. نورالدين، عبد الغني. 2020، الإفصاح المحاسبي عن المخاطر الإلكترونية في ظل المعأيير الدولية للتقارير المالية، مجلة العلوم المالية والمحاسبية، جامعة الجزائر 3، العدد 12.
19. وفاء، بوخاري، وهانية، بوشنافة. 2019، الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ظل معأيير الإبلاغ المالي الدولية: دراسة تحليأتية، مجلة الاقتصاد والأسواق، جامعة المسيلة، العدد 10.
20. يعقوب، ابتهاج إسماعيل، طالب، سلوى، عبد الكريم، هدى، 2022، مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، مجلة العلوم الاقتصادية والإدارية، جامعة بغداد، المجلد 28، العدد 135.
21. يوسف، أحمد جبار. 2022، دور حوكمة تقنية المعلومات في تحسين جودة التدقيق الإلكتروني في ظل التهديدات السيبرانية، جامعة الكوفة، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة.

ثانياً. المصادر الأجنبية:

1. American Institute of Certified Public Accountants (AICPA). 2017. SOC for Cybersecurity: Reporting on an Entity's Cybersecurity Risk Management Program and Controls. .New York: AICPA
2. Benbouali, Dalila, and Siham Berberi. 2018. "Cybersecurity Risk Disclosure in the Financial Sector: A Theoretical and Empirical Approach." Journal of Finance and Accounting Research 10, no. 2.
3. Cormier, Denis, Marie Magnan, and Benoit Van Velthoven. 2009. "Environmental Disclosure Quality in Large German Companies: Economic Incentives, Public Pressures or Institutional Conditions?" European Accounting Review 14, no. 1.
4. COSO. 2020. Enterprise Risk Management: Applying ERM to Cybersecurity, p. 9.
5. Deumes, Rogier, and Wim J. Chel. 2008. "Voluntary Risk Disclosures: Evidence from the Netherlands." .Journal of International Accounting, Auditing and Taxation 17, no. 2
6. ENISA (European Union Agency for Cybersecurity). 2022. Threat Landscape 2022: Impact on Business, p. 17.
7. Grimes, Roger A. 2019. Cybersecurity Program Development for Business. .Wiley
8. Grove, Hugh, and Laurie Schaffner. 2019. "Cybersecurity Governance: A Path to Accountability." Journal of Business and Financial Affairs 8, no. 1: 91–98.
9. Hamm, Susanne J. W. 2019. "The Effects of Cybersecurity Risk Disclosure on Investors' Judgments in Lending Decisions." .Journal of Information Systems 33, no. 2
10. IBM X-Force. 2023. Threat Intelligence Index 2023.
11. IBM. 2023. Cost of a Data Breach Report 2023.
12. ISACA. 2015. Cybersecurity Nexus Glossary. https://www.isaca.org/resources/glossary.
13. Kelton, Andrea S., and Richard R. Pennington. 2020. "The Impact of Cybersecurity Risk Disclosures on Investors' Judgments about the Likelihood of Cyber Incidents and Willingness to Invest.".Journal of Information Systems 34, no. 1
14. Lei, Zheng, Yujie Du, and Fei Xiong. 2019. "Corporate Cybersecurity Risk Disclosure: An Empirical Examination of Determinants and Market Reactions." Journal of Information Security Research 7, no. 1.
15. Luque, Antonio, Carmen de Pablos Heredero, and Álvaro de Pablos Heredero. 2021. "Cybersecurity Disclosure: An Exploratory Analysis of Determinants and Repercussions in the Financial Sector." .Journal of Business Research 132
16. PwC (PricewaterhouseCoopers). 2022. Global Digital Trust Insights. PwC Global.
17. SEC (U.S. Securities and Exchange Commission). Commission Guidance on Public Company Cybersecurity Disclosures. .2018
18. Siegel, Carol A., and Mark Sweeney. 2020. Cyber Strategy: Risk-Driven Security and Resiliency. .Boca Raton, FL: CRC Press, Taylor & Francis Group
19. Verizon. (2022). 2022 Data Breach Investigations Report.
20. Yang, Ying, Jie Ren, and Xuejun Li. 2020. "Cybersecurity Risk Disclosure, Institutional Investors, and Firm Value." (Journal of Corporate Accounting & Finance, 31). (3)