ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

التحديات التي تواجه مراقبة الحسابات في الإفصاح المحاسبي عن المخاطر السيبرانية (دراسة نظرية)

Challenges Facing Auditing in Cyber Risk Disclosure (A Theoretical Study)

الباحثة مروة قتيبة محمد
Researcher: Marwa Qutaiba Mohammed

marwa.qm.off@gmail.com

أ. د. زياد هاشم السقا
Prof. Dr. Ziad Hashim Al-Saqqa

zyad_hashim@uomosul.edu.iq

قسم المحاسبة كلية الإدارة والاقتصاد جامعة الموصل

Department of Accounting, College of Administration and Economics, University of Mosul

تاريخ استلام البحث: 12 / 7 / 2025 **تاريخ قبول البحث: 10 / 9 / 2025**

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

المستخلص

يهدف هذا البحث إلى تسليط الضوء على **التحديات التي تواجه مراقب الحسابات في الإفصاح المحاسبي عن المخاطر السيبرانية**، لما لهذه التحديات من تأثير مباشر على جودة المعلومات المحاسبية، وسلامة التقارير المالية، وشفافية الإفصاح، مما ينعكس على ثقة مستخدمي القوائم المالية.

اعتمد البحث على المنهج الوصفي التحليلي من خلال تحليل الأدبيات السابقة ومراجعة الأدلة المهنية والمعايير الدولية ذات العلاقة، بغية استكشاف أبعاد المشكلة والوقوف على أهم المعوقات التي تواجه المهنة في هذا المجال الحيوي.

وقد خلص البحث إلى أن هناك تفاوت في وعي مراقبي الحسابات بطبيعة المخاطر السيبرانية وحدود مسؤوليتهم تجاهها، مما ينعكس سلبًا على جودة الإفصاح. كما أوصى البحث بضرورة تعزيز دور مراقب الحسابات من خلال تدريب متخصص وإصدار أدلة إرشادية تساعده في تقييم تلك المخاطر والإفصاح عنها.

الكلمات المفتاحية: الإفصاح، المخاطر السيبرانية، مراقبة الحسابات.

Abstract

This research aims to highlight the challenges facing auditors in disclosing cyber risks, given the direct impact these challenges have on the quality of accounting information, the integrity of financial reports, and the transparency of disclosure, which in turn affects the confidence of financial statement users.

The research adopted a descriptive-analytical approach, analyzing previous literature and reviewing relevant professional guidelines and international standards to explore the dimensions of the problem and identify the most significant obstacles facing the profession in this vital area.

The research concluded that there is a disparity in auditors' awareness of the nature of cyber risks and the limits of their responsibility towards them, which negatively impacts the quality of disclosure. The research also recommended strengthening the role of auditors through specialized training and the issuance of guidelines to assist them in assessing and disclosing these risks.

Keywords: Disclosure, Cyber Risks, Auditing

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

اولاً: مقدمة ومشكلة البحث:

في ظل التحوّل الرقمي المتسارع الذي تشهده بيئة الأعمال، أصبحت البيانات والمعلومات المحاسبية هدفاً رئيساً للهجمات السيبرانية التي تهدد سلامة النظم المعلوماتية وجودة الإفصاح المحاسبي. فقد باتت **المخاطر السيبرانية** تمثل تحدياً محورياً أمام مهنة المحاسبة والتدقيق، لا سيما في ظل الاعتماد المتزايد على الأنظمة المحوسبة في إعداد وتقديم القوائم المالية، مما يثير تساؤلات جوهرية حول قدرة نظم الرقابة والتدقيق التقليدية على الاستجابة لتلك التحديات المستحدثة.

ويُعدّ الإفصاح المحاسبي أحد الركائز الأساسية في تعزيز الشفافية والمساءلة، إذ يهدف إلى تمكين مستخدمي القوائم المالية من اتخاذ قرارات رشيدة، غير أن **تعاظم المخاطر السيبرانية** قد يؤدي إلى تشويه أو إخفاء بعض المعلومات، أو التأثير على توقيت وموثوقية الإفصاح عنها. من هنا تبرز أهمية دراسة العلاقة بين الرقابة والتدقيق من جهة، وجودة الإفصاح عن هذه المخاطر من جهة أخرى، خصوصاً مع ضعف الأطر التنظيمية والتشريعية في بعض البيئات المحلية.

إن التحديات الفنية والمهنية والتنظيمية التي تواجه **مراقبي الحسابات** في ظل هذا الواقع الجديد تتطلب إعادة النظر في أساليب وإجراءات التدقيق، وكذلك تطوير أدوات الفحص والرقابة، بما يواكب المخاطر السيبرانية المتغيرة والمعقدة.

وعلى الرغم من إدراك العديد من المنظمات المهنية لأهمية الإفصاح عن المخاطر السيبرانية، إلا أن الواقع المهني في العديد من الدول – ومنها العراق – يُظهر محدودية الإفصاح عن هذه المخاطر في التقارير المالية، فضلاً عن وجود قصور واضح في قدرة مراقبي الحسابات على تقييم تأثيراتها، وبناءً عليه، **تتمثل مشكلة البحث في التساؤل الآتي:**

"هل هناك تحديات تواجه مراقبة الحسابات في الإفصاح المحاسبي عن المخاطر السيبرانية ؟"

ثانياً: اهداف البحث:

يهدف البحث إلى تحقيق عدد من الاهداف المتمثلة بالآتي:

- توضيح المقصود بالإفصاح المحاسبي.
- توضيح المقصود بالمخاطر السيبرانية.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

- تحديد التحديات التي تواجه مراقبة الحسابات في الإفصاح المحاسبي عن المخاطر السيبرانية 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 وتكمن أهمية هذا البحث في تسليطه الضوء على **دور مراقبي الحسابات** في تعزيز **الإفصاح المحاسبي عن المخاطر السيبرانية**، في ظل تنامي التهديدات الرقمية التي تواجه الكيانات الاقتصادية. ويُبرز البحث الحاجة إلى تطوير المعايير والإجراءات الرقابية، ورفع كفاءة المدققين في التعامل مع هذه المخاطر، بما يسهم في **تحسين جودة التقارير المالية، تعزيز الثقة لدى المستخدمين**، ودعم **الاستقرار المالي والمعلوماتي** للمنشآت، والتحديات الجمه التي يواجهها مراقبي الحسابات خصوصاً في البيئة العراقية التي تفتقر إلى بنية تنظيمية واضحة للإفصاح عن الحوادث السيبرانية.

رابعاً: منهج البحث:

اعتمد **البحث على المنهج الاستنباطي** في عرض ومناقشة الدراسات والبحوث والمقالات العلمية المنشورة في المجلات العلمية، وكذلك وضع اساسات نظرية للتحديات التي تواجه مراقبي الحسابات للافصاح عن المخاطر السيبرانية.

خامساً: فرضية البحث:

في ضوء مشكلة البحث واهميته وأهدافه يمكن صياغة فرضية البحث من خلال الاتي: "**هناك تحديات تواجه مراقبة الحسابات في الإفصاح المحاسبي عن المخاطر السيبرانية** ".

المبحث الاول: الإفصاح

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

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 اكثر 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 الافصاح المحاسبي الالكتروني بأنه احد اشكال النشر الالكتروني 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 الافصاح الالكتروني هو النشر الالكتروني على موقع الوحدة الاقتصادية للقوائم والتقارير المالية والايضاحات الاخرى وتقرير مراقب الحسابات الخاص بهدف التأكد من صحة وسلامة المعلومات المنشورة، وسرعة توصيل واتاحة معلومات واضحة ودقيقة لمستخدميها من اصحاب المصلحة، لمساعدتهم في تسهيل عملية اتخاذ القرارات الرشيدة.

ولقد مر الإفصـــاح الإلكتروني بمراحل عدة فكل مرحلة تختلف عن ســـابقتها 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 التســعينات من القرن الماضـــي وقبل ظهور الانترنت اعتمدت الوحدات الاقتصـــادية على ارسال نسخة CD مضغوط تحتوي على المعلومات المالية مرفقة بتقارير مالية ورقية مطبوعة إلى المستفيدين

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

بالبريد، ولكن مع دخول عصر تكنولوجيا المعلومات والانترنت اخذ الافصاح بالتطور (بيومي، 2018،54)، والآتي المراحل التي مرة بها الإفصاح الإلكتروني:

أ. المرحلة الاولى:

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 الا 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 وأخرون، 2017،141).

ب. المرحلة الثانية:

ظهور لغة البرمجة Hypertext Markup وتستخدم اللغة 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).

ت. 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

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 البرنامج الحاسب الذي يُضيف بطاقة تعريفية لكل جزيئة من معلومات القوائم المالية الإلكترونية المُصممة بإستخدام 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 الاخير، تطورت منصات التواصل الاجتماعي في انتاج ونشر معلومات الوحدات الاقتصادية على المنصات، اولاً معظم منصات التواصل الاجتماعي، تقنيات الوصول المباشر (DAIT) التي تدفع بالمعلومات مباشرة إلى المستخدمين بدلاً من مطالبتهم بالبحث عن المعلومات بشكل استباقي، ثانيا تسمح 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 اليها 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 الاخرين، بمعنى اَخر، لا تأتي المعلومات المُتعلقة بالوحدات الاقتصادية في وسائل التواصل الاجتماعي من الوحدات الاقتصادية فحسب، بل تأتي أيضاً من مستخدمي وسائل التواصل الاجتماعي الاخرين، الذين يلعبون دوراً رئيساً في تشكيل الرأي العام (Lei et al,2019,31).

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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

1. وفيها تم البدء في إنشاء مواقع الكترونية للوحدات الاقتصادية، استخدام تقنيات الإنترنت كأحدى الوسائل المستخدمة لنشر التقارير المالية من أبرز ملامح هذه المرحلة قلة عدد الوحدات الاقتصادية وعدم انتظام عملية النشر.
2. تتسم المرحلة الثانية بتزايد عدد الوحدات التي تمتلك مواقع إلكترونية خاصة بها، وتم استخدام الإفصاح الالكتروني بشكل واسع في نشر التقارير المالية المشابهة إلى حد كبير للتقارير المالية المطلوبة.
3. في المرحلة الثالثة ازدادت كمية البيانات المالية وغير المالية المنشورة على الإنترنت بصورة اكبر من التقارير المالية المطبوعة فضلاً عن استخدام طرق مطورة في عرض هذه المعلومات.

وتتمثل أهمية الإفصاح الإلكتروني في اعتقاد منتدى المستشارين في معايير المحاسبة 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 اهمية الإفصاح الالكتروني 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 الى ضرورة زيادة فاعلية دورها في اتخاذ القرارات في هذه الوحدات الاقتصادية.

ويرى الباحثان أنه 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 اليها.

وان للإفصاح الالكتروني اهداف عديدة تتمثل بالآتي (سليمان، 199، 2018):

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 الى 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.

وان لاستخدام تقنية المعلومات في المحاسبة أثر إيجابي على تطوير أساليب المحاسبة والإفصاح المالي من خلال تقديم دقيق للبيانات ومعلومات محاسبية عالية الجودة لمستخدمي التقارير المالية، 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 الالكتروني المرونة اللازمة للمستخدمين في البحث والتصفية والاسترجاع والتنزيل وإعادة تكوين هذه المعلومات.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 وأثارها 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 الإفصـــاح المحاســبي الإلكتروني يمثل حواراً معلوماتياً دائم ومســتمر بين الوحدة وأصحاب المصلحة إذ يمكنهم من تقديم معلومات مُصممة خصيصاً لتلبية الاحتياجات.

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

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 التي تمكن من إمكانية التحقق من صحة المعلومات المنشورة، وتوفير التأمين الكافي للموقع.

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

أ- **عوامل تقنية:** ان 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 الى قارة يحدث في دقائق

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

معدودة وكذلك تدفق المعلومات المحاسبية عِبرَ بيئات الأعمال مما اضطر المؤسسات الى نشر تقاريرها الكترونياً عِبرَ مواقعها.

ب- **عوامل اقتصادية وسياسية:** ان ظهور التجارة الدولية غير الخريطة الاقتصادية والسياسية للعالم إذ ان ابرام الاتفاقيات الزم هذه الدول على حرية دخول رؤوس الاموال والسلعة من دولة الى اخرى ما ادت الى إنشاء أسواق مالية لمواكبة التطورات التي مست التجارة الدولية فقد اصبح ملجأً لتدفق المعلومات بين هذه الدول والاسواق، وظهور ما يعرف بالتجارة الالكترونية مما اضطر المؤسسات إلى الإفصاح الكترونياً عن تقاريرها المالية عبر مواقعها.

ت- **عوامل ثقافية واجتماعية:** إن التقارب الذي حصل بين الشعوب نتيجة لتحسين وتسريع وسائل النقل وكذلك تحسين وسائل الاتصال أدى الى ظهور التسويق العالمي لِمُنتجات المؤسسات وكذلك سهولة الحركة بين هذه الدول ادى الى سهولة حركة اليد العاملة مما جعل الحاجة مَلحة للحصول على معلومات حول المنتجات العالمية وكذلك الحصول على معلومات بيئات الأعمال من اجل البحث عن فرص العمل، كل هذه العوامل أدت إلى ضرورة نشر المؤسسات تقاريرها المالية عِبرَ مواقعها الالكترونية وجعلهُ امراً الزامياً.

ث- **عوامل محاسبية:** إن التطور في مجال المعلوماتية مسَّ كل القطاعات الحيوية الإنسان بما في ذلك الجوانب المحاسبية، إذ ان 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 ان السرعة الفائقة في اداء العمليات الحسابية والمنطقية بدقة متناهية واجراء العديد من الاختبارات الرقابية المبرمجة مسبقاً والقدرة على تخزين كم هائل من البيانات بصور مختلفة كل ذلك ادى الى 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 يتبين أن التطورات والابتكارات التكنلوجية المُستمرة والتشتت الجغرافي لأصحاب المصلحة في الوحدات، والازمات السياسية والاقتصادية التي يمر بها البلاد تؤثر تأثيراً كبيراً على الوضع الاقتصادي بصورة

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

عامة والبيئة الاستثمارية بصورة خاصة، وظهور التجارة الالكترونية والحاجة إلى دخول رؤوس الاموال للبلاد عن طريق مستثمرين اجانب، ان ظهور الانترنت وتوسعهُ حول العالم أدى إلى استخدامهِ في مجال بيئة الاعمال، وظهور المحاسبة الإلكترونية، كل هذه العوامل ادت إلى الحاجة الى 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، فإن 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 (Siegel &Sweeney,2020: 96).

وعرفها (مطر، 2024: 8) بانها مزيج من احتمالية وقوع حدث يهدد شبكة انظمة المعلومات وعواقب هذا الحدث على اصول وسمعه الوحدة، وان احد اسباب المخاطر السيبرانية هي ضعف البنية للشبكات المعلوماتية في الوحدات الاقتصادية وقابليتها للاختراق إذ ان شبكات المعلومات مصممة بشكل مفتوح دون حواجز امنية عليها ورغبة دخول المستخدمين ويمكن استغلال الثغرات الموجودة في الانظمة والشبكات المعلوماتية بهدف التسلل الى البنى المعلوماتية التحتية لاي وحدة اقتصادية وتخريبها (فرحات، 2019: 96).

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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

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

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

ووفقاً لما طرح من اراء يمكن ان توصف المخاطر السيبرانية من قبل الباحثان 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.

في ضوء ما طرح 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 الى هياكل وعمليات فاعلة تمكنها من تحقيق أهدافها.

وباستقراء الفكر فيما يتعلق **بتصنيف المخاطر السيبرانية** التي تواجهها المنشآت، 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

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

البيانات، مسح البيانات السيبرانية أو تشفيرها أو منع الوصول إليها، او الدافع هو الابتزاز، وانقطاع الاتصالات، تعطيل الموقع الالكتروني أو تعطيل الشبكة أو تشويه الموقع للاستيلاء على صفحات وسائل التواصل الاجتماعي والدافع هو الابتزاز أو التجسس.

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

- **المخاطر المتعلقة بتأمين البيانات والمعلومات:** وهي المخاطر الناشئة من تخرين البيانات والمعلومات للأفراد والمؤسسات 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.

وبسبب نمو تقنية الانترنت حصلت الجرائم السيبرانية على اهتمام كبير مقارنة بالجرائم التقليدية إذ يختلف مفهوم الجريمة السيبرانية اختلافا كبيرا عن المفهوم التقليدي للجريمة وذلك بسبب وجود العديد من الخصائص المميزة للجرائم السيبرانية ومن اهم 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 ان يكون لدى الشخص مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال انظمة الحاسب وماهر جدا فيما يتعلق بالأنترنت واجهزة الكمبيوتر.
2. **الامتداد العالمي:** في الفضاء السيبراني لا يوجد حدود وان الجريمة السيبرانية هي جريمة ذات بعد دولي اي انها عابرة للحدود وهذا يعني ان مرتكبي جرائم الامن السيبراني لديهم القدرة على ارتكاب الجرائم عن بعد والتأثير على الضحايا في اي مكان في العالم ويعد هذا احد الخصائص الرئيسة لجرائم الامن السيبراني مما يجعلها تختلف عن جميع انواع الجرائم التقليدية وايضا يجعلها معقدة للغاية.
3. **صعوبة جمع الادلة:** جزء اساس من الافصاح عن الجرائم هو جمع ومعالجة الادلة الرقمية ولكن من الصعب للغاية جمع الادلة فيما يتعلق بالجرائم السيبرانية ويرجع ذلك الى اسباب عديدة على سبيل المثال طبيعة بيانات الكمبيوتر نفسها إذ تعد سريعة الزوال كذلك الامتداد الدولي للجرائم السيبرانية

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

واختلاف القوانين بين الدول وبالتالي هناك صعوبة في التحقق فيها وكذلك اثباتها امام القضاء نظرا لطبيعتها.

4. **حجم اثار جرائم الامن السيبراني لا يمكن تصوره:** تعد جرائم الامن السيبراني اكبر تهديد يواجه المنشآت في الوقت الحالي وواحدة من اكبر التحديات التي ستواجه البشرية وذلك على المدى العقدين المقبلين وبالنسبة للمنشآت فان التكاليف والخسائر المرتبطة بالجرائم السيبرانية ضخمة الى حد لا يمكن تخيله فقد تسبب تلف البيانات او سرقتها، سرقة الاموال، الملكية الفكرية، البيانات الشخصية والمالية، تعطيل اعمال الوحدة بعد تعرضها لهجوم سيبراني كالأضرار بسمعة الوحدة وفقدان الانتاجية وتغير ارقام البيانات في السجلات المخزنة في ذاكرة الحاسبات وغير ذلك من الاثار ويمكن ان تسبب الجرائم السيبرانية في كل ذلك دون ان يكون لها اي اثر خارجي مرئي.

مما سبق يتضح أن **المخاطر السيبرانية** تُشكّل تحديًا كبيرًا يهدد الأفراد والمؤسسات 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 المؤسسات في مختلف القطاعات فإن 82% من الخروقات الأمنية تعود إلى العامل البشري، سواء عبر رسائل التصيّد الاحتيالي أو استخدام كلمات مرور ضعيفة، كما أن غياب التوعية أو ضعف ثقافة الأمن الرقمي يُفاقم هذه المخاطر (Verizon, 2022, 7).

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 المؤسسات 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، وأن الهجمات التي تُشن من خارج المؤسسة 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 والتشغيلية 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 الاثار 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 4.45 مليون دولار للمنشأة الواحدة (IBM, 2023, 8).
2. **انقطاع العمليات التشغيلية:** تؤدي الهجمات السيبرانية إلى توقف الأنظمة الحيوية داخل المنشأة، مما يُعطّل سلسلة التوريد، والمعاملات التجارية، ويؤثر على كفاءة الأداء التشغيلي، وهو ما يُهدد بعجز قصير أو طويل الأجل في تلبية الطلبات.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

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 للمنشأة (ENISA, 2022, 17).
4. **التعرض للمساءلة القانونية والتنظيمية:** في حال عدم التزام المنشأة بالضوابط التنظيمية المتعلقة بحماية البيانات) مثل GDPR أو قوانين الخصوصية المحلية(، فإنها قد تتعرض لغرامات قانونية وعقوبات صارمة، وقد تصل إلى نسب مئوية من الإيرادات السنوية.
5. **زيادة التكاليف التأمينية والتدقيقية:** تؤدي المخاطر السيبرانية إلى ارتفاع في أقساط التأمين على أمن المعلومات، كما تتطلب المنشأة 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 المؤسسات 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 والتشغيلي للمؤسسات، لاسيما مع توسّع الاعتماد على البيئة الرقمية. كما أن 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: تأثير الإفصاح المحاسبي عن المخاطر السيبرانية على مراقبة الحسابات

أولاً: متطلبات الإفصاح عن المخاطر السيبرانية في التدقيق الخارجي

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

في ظل تزايد التهديدات السيبرانية، أصبح الإفصاح عن المخاطر السيبرانية جزءًا أساسيًا من عملية التدقيق الخارجي. تتطلب الهيئات التنظيمية والمعايير الدولية من الشركات تقديم معلومات دقيقة وشفافة حول مخاطرها السيبرانية والإجراءات التي تتخذها لإدارتها. هذه المتطلبات تهدف إلى تعزيز ثقة المستثمرين وأصحاب المصلحة في قدرة الوحدة الاقتصادية على التعامل مع التهديدات السيبرانية والحفاظ على سلامة بياناتها وأصولها.

وفقًا لمجلس معايير المحاسبة المالية (FASB)، يجب على الشركات الإفصاح عن طبيعة ومدى المخاطر السيبرانية التي تواجهها، وتأثير هذه المخاطر على البيانات المالية، والخطوات التي تتخذها لإدارة هذه المخاطر. هذه الإفصاحات يجب أن تشمل تفاصيل حول الحوادث السيبرانية السابقة، وأي تغييرات في سياسات الأمن السيبراني، وأي تكاليف مالية مرتبطة بالهجمات السيبرانية (FASB, 2021, 15)، ومن ناحية أخرة يتطلب مجلس مراقبة المحاسبة العامة (PCAOB) من المدققين الخارجيين تقييم مدى كفاية وفعالية الإفصاحات السيبرانية التي تقدمها الشركات. يجب على المدققين التأكد من أن الإفصاحات تعكس بشكل صحيح المخاطر السيبرانية التي تواجهها الوحدة الاقتصادية وأنها تتوافق مع المعايير المحاسبية الدولية. هذا يشمل التحقق من دقة المعلومات المقدمة، وفحص السياسات والإجراءات الأمنية، وتقييم تأثير الهجمات السيبرانية على البيانات المالية للشركة (PCAOB, 2022, 20)، وعلاوة على ذلك، تتطلب معايير التدقيق الدولية (ISA) من المدققين النظر في المخاطر السيبرانية كجزء من تقييم المخاطر العام للشركة. يجب على المدققين تحليل كيفية تأثير المخاطر السيبرانية على الضوابط الداخلية، وتقييم احتمالية حدوث أخطاء مادية بسبب الهجمات السيبرانية، والتحقق من وجود إجراءات تصحيحية فعالة. هذا يتطلب من المدققين أن يكونوا على دراية بالتقنيات الحديثة والتهديدات السيبرانية الناشئة لضمان إجراء تقييم شامل ودقيق (IAASB, 2023, 25).

ثانياً: التحديات التي تواجه مراقبي الحسابات في الإفصاح عن المخاطر السيبرانية

1. فهم التعقيد التقني

أ. تنوع الهجمات السيبرانية: التنوع في طبيعة وتكرار الهجمات السيبرانية يجعل من الصعب على مدققي الحسابات مواكبة أحدث التهديدات وأساليب الهجوم. يجب على مدققي الحسابات البقاء على اطلاع دائم

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

بالتهديدات الجديدة والناشئة لتقييم فعالية الضوابط الأمنية الحالية. هذا يتطلب مستوى عالٍ من المعرفة التقنية والخبرة في مجال الأمن السيبراني (KPMG, 2024, 3-4).

ب. تكامل الضوابط التقنية مع الإجراءات المالية: يتطلب تقييم الإفصاح عن المخاطر السيبرانية من مدققي الحسابات فهمًا عميقًا لكيفية تكامل الضوابط التقنية مع الضوابط المالية التقليدية، هذا يشمل فهم كيفية تأثير الثغرات الأمنية على البيانات المالية والإجراءات المحاسبية (KPMG, 2024, 3).

2. تقييم الأثر المالي للهجمات السيبرانية

أ. تحديد الأهمية النسبية للهجمات السيبرانية: يجب على مدققي الحسابات تقييم مدى تأثير الهجمات السيبرانية على الأداء المالي للشركة، ويتضمن تحليل الأثر المالي المباشر للهجمات وكذلك الأثر غير المباشر مثل فقدان الثقة من الزبائن والتأثير على سمعة الوحدة الاقتصادية (KPMG, 2024, 5).

وان تحديد الأهمية النسبية للهجمات السيبرانية يعد جزءًا أساسيًا من مهام مدققي الحسابات في العصر الرقمي، والهجمات السيبرانية يمكن أن تتسبب في خسائر مالية كبيرة للشركات، سواء من خلال الأثر المالي المباشر أو التأثيرات غير المباشرة مثل فقدان الثقة من الزبائن والتأثير السلبي على سمعة الوحدة، ولذلك يجب على مدققي الحسابات أن يقوموا بتحليل شامل لهذه الهجمات لتحديد مدى تأثيرها على الأداء المالي للشركة وضمان تقديم تقارير مالية دقيقة وموثوقة فان عليهم:

- يتعين على مدققي الحسابات تقييم الأثر المالي المباشر للهجمات السيبرانية، هذا يشمل تحديد تكلفة الاستجابة للهجمات، مثل إصلاح الأنظمة المتضررة، واستعادة البيانات، وتوظيف خبراء الأمن السيبراني للتعامل مع التهديدات. بالإضافة إلى ذلك، قد تشمل التكلفة المباشرة فديات المدفوعة للقراصنة في حالة هجمات برامج الفدية، والتي يمكن أن تكون مبالغ كبيرة تؤثر على الربحية المالية للشركة (KPMG, 2024, 5).
- يجب على مدققي الحسابات تحليل الأثر غير المباشر للهجمات السيبرانية، والذي يمكن أن يكون أكثر تعقيدًا وتنوعًا. هذا يشمل تقييم تأثير فقدان الثقة من الزبائن، والذي يمكن أن يؤدي إلى خسارة الإيرادات نتيجة انتقال الزبائن إلى منافسين آخرين. سمعة الوحدة قد تتضرر بشكل كبير نتيجة للهجمات السيبرانية، مما يؤدي إلى تراجع قيمة العلامة التجارية وفقدان فرص الأعمال الجديدة. تقرير من PwC

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

يشير إلى أن الشركات التي تتعرض لهجمات سيبرانية كبيرة يمكن أن تفقد ما يصل إلى 20% من قيمتها السوقية في الأسابيع التالية للهجوم بسبب فقدان الثقة والتأثير السلبي على السمعة (PwC, 2022, 12).

- يتعين على مدققي الحسابات أخذ العوامل التنظيمية والقانونية في الاعتبار عند تحديد الأهمية النسبية للهجمات السيبرانية، وعليه فان الشركات قد تواجه غرامات وعقوبات من الهيئات التنظيمية إذا لم تكن تمتثل لمتطلبات الإفصاح عن الحوادث السيبرانية أو إذا فشلت في حماية بيانات الزبائن بشكل كافٍ. هذه الغرامات يمكن أن تكون كبيرة وتؤثر بشكل ملحوظ على الوضع المالي للشركة (Deloitte, 2023, 15)، وأخيرًا، يجب على مدققي الحسابات أن يقوموا بتقييم التأثير على عمليات الوحدة اليومية. الهجمات السيبرانية يمكن أن تعطل الأنظمة والخدمات، مما يؤدي إلى توقف العمليات وفقدان الإنتاجية. هذا يمكن أن يؤثر على الأداء المالي من خلال انخفاض الإيرادات وزيادة التكاليف التشغيلية (EY, 2021, 18).

ب. الاعتماد على الأطر القائمة: يمكن لمدققي الحسابات استخدام أطر تقييم الأهمية النسبية الموجودة لتحديد مدى تأثير الهجمات السيبرانية. هذا يشمل استخدام إطار تحليل المخاطر المعلوماتية (FAIR) لتقييم حجم الخسائر وتحديد التكلفة المالية للهجمات السيبرانية (KPMG, 2024, 5).

3. التعاون مع الفرق الفنية والتنظيمية

أ. التعاون بين فرق الأمن السيبراني والمالية: من المهم أن يتعاون مراقبو الحسابات مع الفرق الفنية والتنظيمية لفهم الإجراءات الأمنية الحالية وكيفية تأثيرها على البيانات المالية، ويجب أن يكون هناك تواصل مستمر بين فرق الأمن السيبراني والفرق المالية لضمان تكامل الإجراءات الأمنية مع الضوابط المالية (KPMG, 2024, 4-5).

ب. توثيق العمليات الأمنية: يجب على مدققي الحسابات التأكد من توثيق جميع العمليات والإجراءات الأمنية بشكل مناسب. هذا يسهل تقييم فعالية الضوابط الأمنية ويضمن استجابة الوحدة بشكل مناسب للهجمات السيبرانية (KPMG, 2024, 6).

4. الامتثال للمتطلبات التنظيمية

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

أ. فهم المتطلبات التنظيمية: يتعين على مدققي الحسابات فهم المتطلبات التنظيمية المتعلقة بالإفصاح عن المخاطر السيبرانية. هذا يشمل متابعة التغييرات في اللوائح والتأكد من أن الشركات تمتثل للمتطلبات الحالية والجديدة (KPMG, 2024, 6).

ب. تقييم مدى امتثال الشركات: يجب على مدققي الحسابات تقييم مدى امتثال الشركات للمتطلبات التنظيمية المتعلقة بالإفصاح عن المخاطر السيبرانية. هذا يشمل فحص السياسات والإجراءات الداخلية والتأكد من أنها تتوافق مع المتطلبات التنظيمية (KPMG, 2024, 7)

5. نقص الإرشادات والمعايير المحددة

ومن التحديات الرئيسية التي يواجهها مراقبو الحسابات عند تقييم الإفصاح عن المخاطر السيبرانية هو نقص الإرشادات والمعايير المحددة التي يمكن الاعتماد عليها. على الرغم من وجود بعض الإرشادات العامة من الهيئات الرقابية مثل مجلس مراقبة محاسبة الشركات العامة (PCAOB) والمجلس الدولي لمعايير المراجعة والتأكيد (IAASB)، إلا أن هذه الإرشادات غالبًا ما تكون غير كافية لتغطية كافة جوانب المخاطر السيبرانية وتقييم تأثيرها المالي بشكل دقيق. على سبيل المثال، يشير مجلس PCAOB إلى ضرورة تقييم المخاطر بشكل مستمر وتحديث الإجراءات بناءً على الأدلة الجديدة، لكن هذه الإرشادات قد لا تتطرق بشكل تفصيلي إلى كيفية التعامل مع التهديدات السيبرانية المتطورة (PCAOB, 2021, 33)، وإضافةً إلى ذلك تفتقر العديد من الشركات إلى توجيهات واضحة بشأن كيفية الإفصاح عن المخاطر السيبرانية في التقارير المالية، مما يجعل من الصعب على مدققي الحسابات التأكد من مدى كفاية ودقة هذه الإفصاحات. نقص المعايير المحددة يعني أيضًا أن هناك تباينًا كبيرًا في كيفية الإفصاح عن المخاطر السيبرانية بين الشركات المختلفة، مما يزيد من صعوبة تقييم هذه الإفصاحات بشكل موحد ومقارنة فعالة بين الشركات (PCAOB, 2008, 34).

6. الاعتماد على متخصصين في الأمن السيبراني

نظرًا لتعقيد وتنوع المخاطر السيبرانية، غالبًا ما يحتاج مراقبو الحسابات إلى التعاون مع متخصصين في الأمن السيبراني لفهم وتقييم هذه المخاطر بشكل دقيق. هذا الاعتماد يمكن أن يشكل تحديًا بحد ذاته،

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

حيث يحتاج المراقبون إلى التأكد من أن هؤلاء المتخصصين يمتلكون الكفاءة والخبرة اللازمة، وأن يتمتعوا بالموضوعية والاستقلالية المطلوبة لضمان تقييم موضوعي وشفاف (PCAOB, 2021, 33).

إضافةً إلى ذلك، يمكن أن يؤدي الاعتماد على متخصصين خارجيين إلى زيادة التكاليف وتعقيد عمليات التدقيق، خاصةً في الحالات التي تتطلب فحصًا مكثفًا وتقييمًا دقيقًا لأنظمة الأمان السيبراني والبنية التحتية التقنية للشركات.

ثالثاً: دور التقنية في تحسين قدرة مراقبي الحسابات على تقييم الإفصاح عن المخاطر السيبرانية

1. تحسين تقييم المخاطر

ان استخدام التقنية المتقدمة مثل الذكاء الاصطناعي وتعلم الآلة يمكن أن يساعد مدققي الحسابات في تحليل كميات كبيرة من البيانات بسرعة وفعالية. تقنيات التحليل التنبؤي يمكن أن تساعد في تحديد الأنماط والاتجاهات التي تشير إلى وجود مخاطر سيبرانية محتملة، مما يتيح للمدققين تقييم المخاطر بشكل أكثر دقة. وفقًا لـ PwC، يمكن أن تسهم أدوات الذكاء الاصطناعي في تحسين دقة التوقعات وتقليل الأخطاء البشرية في عملية تقييم المخاطر (PwC, 2023, 4).

2. الفحص التلقائي وتقييم الضوابط الداخلية

يمكن للتقنية أن تسهل عملية الفحص التلقائي للضوابط الداخلية المتعلقة بالأمن السيبراني، الأنظمة المدمجة يمكن أن توفر تقارير فورية حول حالة الضوابط ومدى فعاليتها، مما يسهل على مدققي الحسابات تقييم الامتثال للمعايير الأمنية. تقرير مركز CAQ يوضح كيف يمكن للتقنية أن توفر رؤى دقيقة ومباشرة حول كفاءة الضوابط الداخلية (CAQ, 2023, 6)

3. تعزيز الشفافية والتواصل

تقنيات مثل منصات إدارة المخاطر يمكن أن توفر وسائل اتصال فعالة بين الإدارات المختلفة داخل الوحدة، مما يعزز الشفافية ويساعد في تحديد المخاطر السيبرانية بشكل أكثر كفاءة. هذه المنصات تسهل أيضًا التوثيق والإبلاغ عن الإجراءات المتخذة لإدارة المخاطر. Deloitte تشير إلى أن استخدام مثل هذه المنصات يمكن أن يحسن من التعاون الداخلي ويسهم في تقليل الفجوات المعلوماتية (Deloitte, 2023, 8).

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

4. أدوات تحليل البيانات الكبيرة

استخدام أدوات تحليل البيانات الكبيرة يمكن أن يساعد مدققي الحسابات في استكشاف البيانات من مصادر متنوعة وتحليلها للكشف عن أي تناقضات أو أنماط غير عادية قد تشير إلى وجود مخاطر سيبرانية. هذه الأدوات تسهل جمع وتحليل البيانات بسرعة ودقة عالية، مما يعزز قدرة المدققين على تقديم تقييمات موثوقة. PwC تؤكد أن الأدوات التقنية المتقدمة تساهم في تقليل وقت التدقيق وتحسين دقته (PwC, 2023, 10).

2-3-7 المسؤولية المهنية لمراقب الحسابات عن المخاطر السيبرانية

أن مسؤولية مراقب الحسابات هي الاطلاع على الأنشطة المتعلقة بالحسابات ومراقبتها من أجل التأكد من سرية وحفظ المعلومات الحساسة في الحسابات، كما ينبغي عليه الحد من تداول معلومات الحسابات الحساسة داخل الشركات أو الوحدات التي يعمل بها مراقب الحسابات ومن أجل تنفيذ هذا الدور بشكل فعال، فإن المدقق الخارجي يقوم بتحديد الحسابات الحساسة وتصنيفها بناءً على حساسية المعلومات المخزنة بها، كما يقوم بضبط الأذونات الخاصة بالوصول إلى هذه الحسابات وتحديد من يمكنه الوصول إليها ومن لا يمكنه؛ وفي حال اكتشاف أي انتهاك لسياسة الحسابات أو اكتشاف أي نشاط غير عادي، فإن مراقب الحسابات يجب أن يتخذ الإجراءات اللازمة بسرعة لإجراء التحقيقات اللازمة وتحديد السبب والمسؤول عن ذلك (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة، 2005، 274)

ومن الجدير بالذكر أن مراقب الحسابات ليس المسؤول الوحيد عن تحقيق سياسات أمن البيانات أو الوحدة، ولكنه يعتبر جزءا مهماً من الفريق الذي يعمل على تحقيق هذه السياسات وتحديد المخاطر المحتملة.

وأشار معيار التدقيق الدولي بالرقم 4000 بأنه يجب على مراقب الحسابات القيام بتقييم المخاطر الجوهرية ومخاطر الرقابة للجوانب المادية في البيانات المالية في بيئة نظام المعلومات الالكتروني وذلك لأنها ربما يكون لها تأثير احتمالي عام وخاص على الأخطاء الجوهرية للبيانات المالية (Elifoglu, 67-71, 2002).

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

كما وأشار نفس المعيار الدولي في الفقرة 33 انه في بيئة نظام معلومات يستخدم الحاسوب فانه لا تتغير أهداف اختبارات الرقابة عنها في البيئة اليدوية ومع ذلك فان بعض إجراءات التدقيق قد تتغير وقد يجد المراقب نفسه مضطرا أو قد يفضل استعمال طرق التدقيق بمساعدة الكومبيوتر (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة، 2005، 275).

كما أشار معيار التدقيق الدولي رقم 401 في الفقرة 12 على ما يلي: أن أهداف مراقب الحسابات الخاصة لا تتغير في حالة معالجة المعلومات المحاسبية يدويا أو الكترونيا ومع ذلك فان طرق تطبيق إجراءات التدقيق لجمع الأدلة قد تتأثر بطرق معالجة الحاسوب ويستطيع المراقب استعمال الإجراءات اليدوية للتدقيق أو طرق التدقيق بمساعدة الكومبيوتر أو استعمال الطريقتين معا لغرض الحصول على أدلة كافية". ومع: ذلك فإنه قد يكون من الصعب أو المستحيل على المراقب في النظم المحاسبية التي تستخدم الكومبيوتر لمعالجة تطبيقات مهمة أن نحصل على معلومات معينة لفحصها أو للاستفسار عنها أو للتأكد منها بدون مساعدة الكومبيوتر (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة 2005: 287).

وأصدر المجلس الأمريكي ASB معيار التدقيق (80) SAS في كانون أول 1996 كمتطلب إثبات ليعالج المسائل المتعلقة بصلاحية واكتمال وتكامل الدليل الالكتروني في نظام مراقبة تكنلوجيا المعلومات" (Helms & Lilly, 2000, 2).

إذا عندما تقوم الشركات بنقل عملية أو تخزين أو الوصول إلى معلومات الكترونيا فانه من غير العملي أو حتى من المستحيل تخفيض المخاطر بمستوى منخفض وبشكل مقبول فقط بواسطة إجراء اختبارات عينية لواحدة أو أكثر من البيانات المالية، كما أن المعيار (80) SAS يستنتج إن اختبارات الرقابة مع الاختبارات العينية يجب أن تكون كافية لتدعيم نتيجة التدقيق دراسة إجراءات التدقيق من قبل المجلس الأمريكي ASB قد وضعت الدليل الالكتروني إن وأمور التقييم المرتبطة به كما لم يجر أي تحديث رغم إن بعض الأحكام الإرشادية قد عالجت بعض الاعتبارات المحاسبية في مجال تقنية المعلومات لتقييم الرقابة منذ صدور المعيار (SAS 78) إلا أن المعيار الجديد (SAS 94) ملا هذه الفجوة لتحقيق أهداف معينة، حيث انه ومع إدراك أهمية تقنية المعلومات جاء المعيار الجديد معدلا للمعيار (55) SAS ولكنه لم يغير

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

المبادئ الأساسية له ولم يغير أهميته كنموذج لمخاطر التدقيق ولكنه عالج آثار التقنيات على إجراءات المعايير الفنية (Helms & Lilly 2000, 54).

المحور الرابع: الاستنتاجات والتوصيات

أولاً: الاستنتاجات

1. ضعف المعايير الخاصة بالإفصاح عن المخاطر السيبرانية: يتبين أن غياب إطار معياري ملزم للإفصاح المحاسبي عن المخاطر السيبرانية أدى إلى تباين كبير في مستوى الإفصاح بين الشركات، مما أثّر سلبًا على شفافية القوائم المالية وقلل من قدرتها على تلبية احتياجات مستخدمي المعلومات المحاسبية.
2. قصور دور مراقبي الحسابات في التحقق من الإفصاح السيبراني: أظهرت النتائج أن مراقبي الحسابات يواجهون صعوبات فنية ومهنية في تقييم كفاية وصدق الإفصاح عن المخاطر السيبرانية، ويرجع ذلك إلى نقص التدريب المتخصص، وضعف إدماج تقييم المخاطر التكنولوجية ضمن خطط التدقيق التقليدية.
3. تأثير محدود للإفصاح السيبراني على قرارات المستثمرين: رغم الأهمية المتزايدة للمخاطر السيبرانية، إلا أن مستوى الإفصاح الحالي عنها لم يصل بعد إلى درجة تؤثر بفعالية على قرارات المستخدمين الخارجيين، بسبب غموض أو عمومية البيانات التي يتم الإفصاح عنها وعدم تقييسها بمؤشرات كمية واضحة.

ثانياً: التوصيات

1. تطوير إطار معياري خاص بالإفصاح السيبراني: توصي الدراسة بضرورة قيام الهيئات المحاسبية الدولية والوطنية، مثل IASB وIFAC، بتبني إطار موحد للإفصاح عن المخاطر السيبرانية، يتضمن مؤشرات كمية وكيفية، ويوفر إرشادات لمراقبي الحسابات حول طبيعة الاختبارات والإجراءات اللازمة.
2. تعزيز كفاءة مراقبي الحسابات بالتدريب التخصصي: يجب إدراج موضوعات الأمن السيبراني والإفصاح المحاسبي عنه ضمن برامج التأهيل المهني لمراقبي الحسابات، مع توفير أدلة عمل تدقيقية مرتبطة بأنواع الهجمات السيبرانية وتقدير احتمالات تحققها وتأثيرها المالي.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

3. فرض إفصاح دوري إجباري عن الحوادث السيبرانية: ينبغي على الجهات الرقابية فرض إلزام قانوني على الشركات للإفصاح الدوري والمفصل عن الحوادث السيبرانية التي تتعرض لها، والإجراءات المتخذة لمعالجتها، بما يعزز ثقة مستخدمي القوائم المالية ويعزز فاعلية دور التدقيق الخارجي في هذا المجال.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

المصادر

1. البغدادي، السيد أحمد عبد المقصود، 2021، **الحوكمة الرقمية والأمن السيبراني: إطار متكامل لإدارة المخاطر في المؤسسات 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 تحليلية تطبيقية، **المجلة العراقية للعلوم الإدارية**، المجلد 7، العدد 27.
5. 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.
6. 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.
7. السواح، حسام عبد الله. 2021، دور التدقيق الداخلي في إدارة مخاطر الأمن السيبراني: دراسة تحليلية تطبيقية، **مجلة البحوث المحاسبية**، جامعة الإسكندرية، المجلد 22، العدد 4.
8. شحاته، أحمد عبد المنعم، البردان، حسين، 2021، أثر تطبيق معايير الإفصاح عن المخاطر على جودة التقارير المالية في ظل التهديدات السيبرانية، **مجلة البحوث المالية والتجارية**، جامعة الأزهر، العدد 2، مصر.
9. 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.
10. فرحات، عبد الرزاق. 2019، **الأمن السيبراني ودوره في حماية المعلومات في البيئة الرقمية**، دار صفاء للنشر والتوزيع، الأردن.

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

11. القزاز، مازن أحمد، السقا، زياد هاشم، 2019، أثر ممارسات الحوكمة في تقليل مخاطر الأمن السيبراني: دراسة تحليلية في البيئة الجامعية العراقية، **مجلة تنمية الرافدين**، المجلد 41، العدد 3.

12. الكرعاوي، أحمد جاسم محمد. 2024، الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ضوء المعايير الدولية للتقارير المالية: دراسة تطبيقية، **جامعة الكوفة**، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة، العراق.

13. محسن، محمد عبد اللطيف، وآخرون. 2017، تأثير الإفصاح عن المخاطر غير المالية على جودة التقارير المالية في ظل المعايير الدولية، **مجلة المحاسبة والمراجعة**، كلية التجارة، جامعة القاهرة، العدد 45.

14. مطر، نزار. 2024، **التدقيق السيبراني كمدخل لتعزيز فعالية أنظمة الرقابة الداخلية في الوحدات الاقتصادية**، دار الكتاب الأكاديمي، لبنان.

15. نورالدين، عبد الغني. 2020، الإفصاح المحاسبي عن المخاطر الإلكترونية في ظل المعايير الدولية للتقارير المالية، **مجلة العلوم المالية والمحاسبية**، جامعة الجزائر 3، العدد 12.

16. وفاء، بوخاري، وهانية، بوشنافة. 2019، الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ظل معايير الإبلاغ المالي الدولية: دراسة تحليلية، **مجلة الاقتصاد والأسواق**، جامعة المسيلة، العدد 10.

17. 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.
18. Center for Audit Quality (CAQ). 2023. Technology in Audit Practice. CAQ Reports.
19. 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.
20. COSO. 2020. Enterprise Risk Management: Applying ERM to Cybersecurity, p. 9.
21. Deloitte. 2023. Cyber Risk Frameworks and Regulatory Compliance. .Deloitte Insights
22. ENISA (European Union Agency for Cybersecurity). 2022. Threat Landscape 2022: Impact on Business, p. 17.
23. EY (Ernst & Young). 2021. Cybersecurity and Financial Integrity. EY Global.
24. Grimes, Roger A. 2019. Cybersecurity Program Development for Business. .Wiley

ISSN: 2392- 5418 e-ISSN: 2520- 7423 DOI:10.59799/SQZH5356

25. Helms, Marilyn M., and Bryan Lilly. 2000. "Electronic Audit Evidence: SAS 80 and Beyond." .Journal of Accountancy

26. IBM X-Force. 2023. Threat Intelligence Index 2023.

27. IBM. 2023. Cost of a Data Breach Report 2023.

28. ISACA. 2015. Cybersecurity Nexus Glossary. https://www.isaca.org/resources/glossary.

29. KPMG. 2024. Cybersecurity Risk and Audit Challenges. .KPMG Insights

30. 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.

31. Public Company Accounting Oversight Board (PCAOB). 2022. Cybersecurity and the External Audit. .PCAOB

32. PwC (PricewaterhouseCoopers). 2022. Global Digital Trust Insights. PwC Global.

33. SEC (U.S. Securities and Exchange Commission). Commission Guidance on Public Company Cybersecurity Disclosures. .2018

34. Siegel, Carol A., and Mark Sweeney. 2020. Cyber Strategy: Risk-Driven Security and Resiliency. .Boca Raton, FL: CRC Press, Taylor & Francis Group

35. Verizon. (2022). 2022 Data Breach Investigations Report.