العلاقة بين اختراقات الأمن السيبراني والافصاح عنها وقرار الاستثمار في الشركات المصرية والدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني ـ دراسة تجريبية

أ.م.د. أحمد محمد شوقي محمد فهمي توفيق*

(*) أ.م.د. أحمد محمد شوقي محمد فهمي توفيق: أستاذ المحاسبة والمراجعة المساعد كلية الأعمال – جامعة الإسكندرية

Email: ahmed.shawki@alexu.edu.eg
ahmedmohamedshawki@gmail.com

ملخص:

هدف البحث إلى تحليل واختبار الأثر المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين اختراقات الأمن السيبراني والافصاح عنها، وقرار الاستثمار في الشركات المصرية. واعتمد الباحث على تصميم تجريبي (٢x٢x٢) لعينة من ٥٢ من الأكاديميين وطلاب الدراسات العليا كممثلين عن المستثمرين غير المحترفين، مع إجراء تحليل إضافي عن العوامل المؤثرة على الإفصاح عن الاختراقات السيبرانية، والعوامل المؤثرة على الإفصاح عن إدارة مخاطر الأمن السيبراني.

وتوصلت النتائج إلى وجود أثر سلبي معنوي لكل من الاختراقات السيبرانية والإفصاح عن اختراقات الأمن السيبراني على قرار وقيمة الاستثمار بالشركات المصرية، ووجود أثر سلبي غير معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات، بينما اتضح وجود أثر معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات.

كما خلصت نتائج التحليل الإضافي إلى أهمية كل من مستوى الثقة في مجلس الإدارة، ومدى أهمية الشركة في القطاع الذي تعمل به، وقوة نظام الرقابة الداخلية في الشركة التي تم اختراقها، على الإفصاح عن الاختراقات السيبرانية. كما اتضح أهمية أثر وجود قصور في نظام الرقابة الداخلية، وعدم وجود مراجع خارجي مستقل للتوكيد على أنظمة الشركة على زيادة احتمال وقوع الاختراقات السيبرانية بالشركة. كما أوضحت نتائج التحليل الإضافي إلى أهمية كل من وجود قوانين أو لوائح منظمة، ووجود سياسات واضحة لإدارة مخاطر الأمن السيبراني، والاستثمارات في إدارة مخاطر الأمن السيبراني بالشركة، وقوة النظم الرقابية بالشركة على الافصاح عن إدارة المخاطر السيبرانية. كما أشارت نتائج الدراسة أن أكثر القطاعات أهمية للإفصاح عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني هو القطاع المالي والبنكي ثم قطاع الاتصالات.

الكلمات المفتاحية: الاختراقات السيبرانية– الإفصاح عن الاختراقات السيبرانية– الإفصاح عن إدارة مخاطر الأمن السيبراني –قرار الاستثمار

The Relationship Between Cybersecurity Breaches, and their Disclosure on Investment Decisions in Egyptian Companies, and the Moderating Role of Cybersecurity Risk Management Disclosure - An Empirical Study

Abstract:

The research aims to analyze and test the moderating effect of disclosing cybersecurity risk management on the relationship between cybersecurity breaches and their disclosure, and the investment decision in Egyptian companies. The researcher relied on a (2x2x2) experimental design for a sample of 52 academics and graduate students as representatives of non-professional investors, with additional analysis of the factors affecting the disclosure of cyber breaches, and the factors affecting the disclosure of cybersecurity risk management.

The results showed a significant negative impact of both cyber breaches and their disclosure on the investment decision and value of Egyptian companies. There was a non-significant negative impact of the moderating role of cybersecurity risk management disclosure on the relationship between cyber breaches and investment decisions. Moreover, A significant impact of the moderating role of cybersecurity risk management disclosure on the relationship between cyber breaches disclosure and the investment decision and value of the companies

Furthermore, the additional analysis results concluded the importance of the level of confidence in the board of directors, the company's importance in its operating sector, and the strength of the internal control system in the breached company, on cyber breach disclosure. The results indicated the importance of the weakness effect in the company's internal control system and the absence of an independent external auditor verifying the company's systems in increasing the likelihood of cyber breaches in the company. The study also concluded the importance of having strict laws or regulations, detailed policies for cybersecurity risk management, the investment in cybersecurity risk management in the company, the strength of the company's control systems on the disclosure of cybersecurity risk management. The study's results also indicated that the most important sectors for cyber breaches and cybersecurity risk management disclosures are the financial and banking sectors, followed by the telecommunications sector.

Keywords: **Cybersecurity Breaches, Cybersecurity Breach Disclosure, Cybersecurity Risk Management Disclosure-Investment Decision**.

١/مقدمة:

أدت الاختراقات السيبرانية Cybersecurity breaches and incidents العالمية إلى جذب انتباه المشرعين والهيئات المهنية بخصوص أهمية افصاح الشركات عن الاختراقات السيبرانية Cybersecurity breaches disclosure (CBD) وفعالية نظم إدارة المخاطر السيبرانية Cybersecurity risk management في تخفيض تلك المخاطر. وصاغت عدد من الدول المتقدمة قوانين ولوائح خاصة بالإفصاح عن إدارة المخاطر بصفة عامة وعن الاختراقات السيبرانية بصفة خاصة، (Securities and Exchange Commission,(SEC) (2017,2022; Cheng et al. 2022. وأوضحت تلك اللوائح وجود إلزام للشركات المتداولة ببعض البورصات بالإفصاح عن حوادث الاختراق السيبراني، كما في البورصات الأمريكية (Goel and Shawky, 2023).

كما اهتمت الهيئات بتنظيم إطار إدارة المخاطر السيبرانية والإفصاح عن الاختراقات السيبرانية، حيث قامت لجنة COSO (2017) بتحديث إطار إدارة المخاطر المؤسسية Enterprise Risk Management (ERM) ليتضمن تحسين إدارة المخاطر السيبرانية والإفصاح عن عوامل الخطر السيبراني والإشراف على فريق لتقييم وإدارة المخاطر السيبرانية والاستثمار في التدريب السيبراني مع دمج إدارة المخاطر السيبرانية في خطة الشركة الاستراتيجية، والإفصاح عن المعلومات المتعلقة بالاختراقات السيبرانية للأطراف ذات الصلة. كما قدمت جمعية المحاسبين القانونيين الأمريكية AICPA (2017a) وصف لإجراءات إدارة المخاطر السيبرانية، بالإضافة إلى إطاراً للتقرير عن إدارة مخاطر الأمن السيبراني ومعايير للأمن السيبراني AICPA,SOC(2017b) والذي يساعد الشركات على توصيل المعلومات الملائمة والمفيدة عن الأمن السيبراني. وحدد الإطار وصف للمعلومات الهامة وإفصاحات الإدارة عن مدى فعالية نظم الرقابة في مقابلة أهداف الأمن السيبراني مع وجود تصديق من مراجع خارجي مستقل. وتضمن التقرير عن إدارة مخاطر الأمن السيبراني **ثلاثة جوانب أساسية** هي؛ وصف برنامج إدارة الأمن السيبراني، وتأكيدات الإدارة عن فعالية أنظمة الرقابة الداخلية لتحقيق أهداف الأمن السيبراني، ورأي المراجع المستقل عن فعالية أدوات الرقابة الداخلية لتحقيق أهداف الأمن السيبراني بالشركة. كما تضمن الإطار **مجموعتين** من المعايير تتضمن **معايير وصف برنامج إدارة المخاطر**

السيبرانية بواسطة الشركة، **ومعايير الرقابة** التي تستخدم لتقييم فعالية نظم الرقابة في برنامج إدارة المخاطر السيبرانية.

كما حددت هيئة الأوراق المالية الأمريكية (2018) SEC افصاح الشركات المساهمة عن اجراءات الأمن السيبراني من خلال تقديم معلومات مستمرة وفي الوقت المناسب في التقارير الدورية مثل 10–K–or 10—Q ، دون وجود أي مهلة زمنية على الشركات لتقوم بالإفصاح عن حوادث الأمن السيبراني المهمة.

كما أصدرت هيئة الأوراق المالية الأمريكية (2022)SEC تعديلات علي قواعدها بشأن متطلبات الإفصاح المتعلقة بإدارة مخاطر الأمن السيبراني ليشمل الإفصاح عن حوادث الاختراقات السيبرانية غير الجوهرية والتي يمكن أن تصبح جوهرية، وإعداد تقرير حول سياسات استجابة الإدارة للحوادث السيبرانية وتقييم الأهمية النسبية للحوادث السيبرانية والإفصاح بشكل دوري عن الاستراتيجية و السياسات والاجراءات المتبعة في حوكمة المخاطر السيبرانية والمسئول عنها، وطلبت الهيئة من الشركات العامة الإفصاح عن حوادث الأمن السيبراني المهمة في **خلال أربعة أيام** عمل من اكتشافها من خلال تقديم نموذج 8–K.

وأشارت بعض الدراسات المحاسبية (De Arroyabea and De Arroyabe 2021; Sari et al. 2024) إلى وجود أثار سلبية للاختراقات السيبرانية على قيمة الشركة وسمعة الشركة وقرارات المستثمرين المحتملين في تلك الشركات. كما اهتمت بعض الدراسات المحاسبية (Kelton and Pennington 2020; Li et al.2021; Demk and Kaplan 2023) بالدور الايجابي للإفصاح عن إدارة مخاطر الأمن السيبراني وإجراءاتها في تخفيض أو الحد من أثار الاختراقات السيبرانية على قيمة الشركات والاستثمار بها. بينما أوضحت دراسة(شرف ٢٠٢٣ ; Romanosky and Sayers,2024) انخفاض الأثر الايجابي لإدارة مخاطر الأمن السيبراني والإفصاح عنها على تخفيض الأثر السلبي للاختراقات السيبرانية.

وفي نفس السياق، قام البنك المركزي المصري (٢٠٢٣) بإنشاء مركز الاستجابة للإبلاغ عن حوادث الأمن السيبراني، والتصيد والاحتيال الالكتروني (EF–FinCIRT) وذلك للإبلاغ عن الهجمات الإلكترونية التي تشكل تهديداً لاستقرار الأمن السيبراني بالبنوك، وبهدف المساعدة في الوقاية والتصدي للمخاطر والاختراقات الأمنية ومنع تكرارها داخل القطاع المالي والمصرفي. كما

يقوم البنك المركزي المصري بالكشف عن العديد من الهجمات السيبرانية بصورة استباقية من خلال الترابط بين البنوك والمؤسسات المالية للمساعدة في الكف عن المخاطر الأمنية وابلاغ الجهة المهددة بصورة مبكرة لاتخاذ اجراءات الأمن السيبراني اللازمة وفقا لحدة وخطورة الاختراقات السيبرانية المحتملة، مع تحديد الاجراءات المضادة الموصي باتخاذها. كما تم اصدار إطار للأمن السيبراني التنظيمي لتعزيز سياسات التقييم الذاتي والحفاظ على بيئة عمل وبنية تحتية تكنولوجية تتمتع بأعلى درجات الأمن السيبراني.

وبالرغم من الاهتمام الدولي بالإفصاح عن الاختراقات السيبرانية وادارة المخاطر السيبرانية واهتمام البنك المركزي المصري بإنشاء مركز الاستجابة للإبلاغ عن حوادث الأمن السيبراني وإطار الأمن السيبراني التنظيمي، إلا أنه لا يوجد تقنين للإفصاح عن الاختراقات السيبرانية أو إدارة مخاطر الأمن السيبراني **في جمهورية مصر العربية**، كما لا توجد أية معايير محاسبية أو معايير مراجعة مصرية تناولت هذا الإفصاح بصورة مباشرة، ولازال هذا الإفصاح عن إدارة مخاطر الأمن السيبراني في مصر بصورة اختيارية. ولا توجد أية متطلبات من سوق الأوراق المالية المصرية للشركات المقيدة بالبورصة بتقديم مثل هذا النوع من الإفصاح(علي، وعلى ٢٠٢٢).

وبناء على ما سبق، يتضح عدم وجود إلزام بالإفصاح عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني في جمهورية مصر العربية، وندرة الدراسات المحاسبية الخاصة بالدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والإفصاح عنها وقرار الاستثمار في الشركات المصرية بما يعد دافعاً لهذا البحث.

٢/ مشكلة البحث:

اهتمت الدراسات المحاسبية باختبار أثر اختراقات الأمن السيبراني والإفصاح عنها على قرار الاستثمار في الشركات (Tweneboah–Kouda et al 2018; Cheng et al. 2022; Huang and Murthy2024) إلا أن الدراسات لم تركز بدرجة كافية على الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين اختراقات الأمن السيبراني والإفصاح عنها وقرار الاستثمار في الشركات المصرية. وبناء على ما سبق، يمكن صياغة مشكلة البحث في الإجابة على الأسئلة التالية:

- هل تؤثر اختراقات الأمن السيبراني على قرار الاستثمار في الشركات المصرية؟
- هل يؤثر الإفصاح عن اختراقات الأمن السيبراني على قرار الاستثمار في الشركات المصرية؟

- هل يؤثر الافصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات المصرية؟
- هل يؤثر الافصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار الاستثمار في الشركات المصرية؟

٣/ هدف البحث:

يهدف هذا البحث إلى تحليل واختبار العلاقة بين اختراقات الأمن السيبراني والإفصاح عنها وقرار الاستثمار في الشركات المصرية، وتحليل الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على هذه العلاقة في الشركات المقيدة في البورصة المصرية

٤/ أهمية البحث

تتضح **أهمية البحث العلمية** من تحليل أثر الاختراقات السيبرانية والافصاح عنها على قرار الاستثمار في الشركات المصرية والدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على هذه العلاقة، ومعالجة الفجوة البحثية في الدراسات ذات الصلة.

كما يستمد البحث أهميته **العملية** بإيجاد دليل تطبيقي على أثر اختراقات الأمن السيبراني والإفصاح عنها على قرارات أصحاب المصالح للاستثمار في الشركات، وأثر الافصاح عن إدارة المخاطر السيبرانية على تلك العلاقات، بما ينعكس إيجابا على أصحاب المصالح المختلفة في تلك الشركات، والمشرعين عند صياغة الارشادات واللوائح عن إدارة مخاطر الأمن السيبراني ومقاومة الاختراقات السيبرانية للشركات.

وترجع **دوافع البحث** إلى أثر الاختراقات السيبرانية والافصاح عنها على سلامة واستمرارية الأنظمة الإلكترونية بالشركات، وتأثيرها على المراكز المالية لها، ودور إدارة مخاطر الأمن السيبراني في تخفيض أثار الاختراقات السيبرانية وأهميتها بالنسبة لأصحاب المصالح المختلفة بالشركات، وأثرها على استجابة المستثمرين في تلك الشركات.

٥/ حدود البحث

يقتصر نطاق البحث على الاختراقات السيبرانية والإفصاح عنها، والدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني داخل الشركات، وبالتالي لن يتم التعرض للعوامل المؤثرة على فعالية إدارة المخاطر السيبرانية مثل الخلفية التعليمية لأعضاء مجلس الإدارة ونوع العضو

ومكافآت أعضاء مجلس الإدارة، وأثر تقرير المراجع المستقل على تلك الإفصاحات إلا بالقدر الذي يلزم لتناول مشكلة البحث بصورة علمية ومنطقية. وتعتبر قابلية النتائج للتعميم مشروطة بضوابط اختيار عينة الدراسة.

٦/خطة البحث

١. الاختراقات السيبرانية والإفصاح عنها – المفهوم والمردود الاقتصادي
٢. الأمن السيبراني، وإدارة مخاطر الأمن السيبراني والإفصاح عنها: المفهوم والمردود الاقتصادي.
٣. تحليل الدراسات المحاسبية الخاصة بالعلاقة بين الاختراقات السيبرانية والافصاح عنها وقرار الاستثمار في الشركات
٤. الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين اختراقات الأمن السيبراني والإفصاح عنها وقرار الاستثمار في الشركات
٥. منهجية البحث
٦. نتائج اختبار فروض البحث
٧. النتائج والتوصيات ومجالات البحث المقترحة

٦/١- الاختراقات السيبرانية والإفصاح عنها – المفهوم والمردود الاقتصادي

اهتمت الدراسات المحاسبية (Sundareswaran et al. 2018; Caladarula et al.2022; Srinivas and Huigang 2022) **بمفهوم الاختراقات السيبرانية cybersecurity Breaches** والإفصاحات عنها وأثارها الاقتصادية. فقد عرفت دراسة Sundareswaran et al. (2018) الاختراقات السيبرانية بأنها تهديدات للبيانات نتيجة نقاط ضعف في إمكانيات النظم الآلية وعدم قدرتها على منع تسرب وسرقة البيانات. كما عرفت دراسة (Gao.,2016; Caladarula et al.2022) الحوادث أو الاختراقات السيبرانية بأنها أحداث تهدد من ثقة وسلامة وتوافر أنظمة المعلومات الالكترونية بالشركات سواء بصورة مقصودة أو غير مقصودة بما يؤدي لخسائر اقتصادية ومرتبطة بسمعة الشركة.

وفي نفس السياق، عرفت دراسة Furnell and Dowling (2019) حوادث الأمن السيبراني بأنها مجموعة من الاختراقات التي تتم عن طريق الحاسب الآلي وشبكات الأنترنت مثل انتشار

الفيروسات والبرامج الضارة بما يؤدي لتعطل الأجهزة والبرامج عن أداء الخدمات مثل توقف خوادم الأنترنت عن العمل وتعطل شبكة الانترنت والمواقع الإلكترونية.

كما عرفت دراسة Srinivas and Huigang (2022) الاختراقات السيبرانية بأنها جرائم تخص البيانات وأنظمة الشركات بصورة مقصودة أو غير مقصودة بما يؤدي لعدم الثقة في بيئة البيانات الخاصة بالشركة، وتشمل تسرب البيانات والإفصاحات غير المقصودة للبيانات، وانتشار البيانات غير الصحيحة عن الشركات.

وبالتالي يمكن للباحث **تعريف الاختراقات السيبرانية** بأنها: **جرائم أو تهديدات نتيجة نقاط ضعف بأنظمة الشركات، بما يؤدي لتسرب وسرقة البيانات وإتلاف النظم، سواء بصورة مقصودة أو غير مقصودة، بما يؤدي لخسائر اقتصادية وخسائر لسمعة الشركات.**

وبشأن الإفصاح عن الاختراقات السيبرانية، اهتمت هيئة الأوراق المالية الأمريكية SEC (2017) بفحص ومراجعة إفصاحات الشركات عن مخاطر الأمن السيبراني والسياسات واجراءات الرقابة لمواجهة التهديدات السيبرانية، مع إلزام الشركات بالإفصاح عن مخاطر الاختراقات السيبرانية و التي تؤثر على مخاطر الاستثمار في تلك الشركات.

كما أوضحت دراسة Andrew et al.(2023) تأثير الافصاح عن الاختراقات السيبرانية على مسائلة إدارة الشركات داخل سوق المال الاسترالي، وبما ساهم في تحديد القواعد المنظمة للحد الأدنى للإفصاح عن اختراقات البيانات وفق تشريعات الحكومة الاسترالية ويشمل الحد الأدنى للإفصاحات عن الاختراقات السيبرانية؛ (محددة أو غير محددة)، وحساسية البيانات التي تم اختراقها (بيانات شخصية أو شخصية تؤدي لأضرار بالشركة)، و اسباب الاختراق السيبراني (خطأ بشري أم هجوم سيبراني)، وحجم الاختراق السيبراني و عدد المتأثرين به، و تاريخ الافصاح عن الاختراقات السيبرانية وطريقة الاختراق السيبراني، وأثر قوانين الافصاح عن الاختراقات السيبرانية أو القوانين المتأثرة بتلك الاختراقات، واستراتيجيات تخفيض مخاطر الاختراقات السيبرانية.

وفي نفس السياق أشارت دراسة Guo and Fluharty (2024) إلى أنه على الرغم من اختلاف تفاصيل قوانين الإفصاح عن الاختراقات السيبرانية Data Breaches Disclosure (DBD) من ولاية أمريكية إلى أخرى، إلا أن هذه القوانين بشكل عام تتطلب من الشركات التي تتأثر باختراقات البيانات إعلان الأفراد والكيانات المتضررة بحدوث اختراق البيانات، وأنه عادةً ما

تحتوي قوانين الولاية على أحكام تفصيلية تحدد نطاق الاختراق ومتطلبات الإفصاح والجداول الزمنية للإخطار والعقوبات المتعلقة بعدم الالتزام بالإفصاح عن اختراقات البيانات، وإجراءات تنفيذها. وعلى الرغم من أن الإفصاح المطلوب يقتصر على الأفراد المتضررين، إلا أنه لا يزال من المحتمل أن يكون واسع النطاق لأن العديد من الأفراد يتأثرون بتلك الاختراقات. كما أشارت الدراسة إلى زيادة عدد الحوادث التي تم الإبلاغ عنها بشكل كبير بعد إلزام الشركات بقوانين الافصاح عن الاختراقات السيبرانية.

وبناء على ما سبق، يمكن للباحث تعريف **الإفصاح عن الاختراقات السيبرانية** بأنه: **مجموعة من الإفصاحات الإلزامية من جانب الشركات التي تعرضت لاختراقات أو تهديدات سيبرانية، تقدم للهيئات الحكومية للرقابة على الشركات المسجلة في البورصات بشأن نوع الاختراقات السيبرانية وطبيعتها وأسبابها وطرقها والمتأثرين بتلك الاختراقات، ومدى تأثير القوانين على تخفيض تلك الاختراقات.**

وبشأن المردود الاقتصادي لاختراقات الأمن السيبراني والإفصاح عنها، فقد اهتمت بعض الدراسات المحاسبية بالأثر الاقتصادي لاختراقات الأمن السيبراني والإفصاح عنها، فأوضحت دراسة Sundareswaran at al. (2018) وجود نتائج اقتصادية جوهرية نتيجة اختراقات البيانات مثل سوء استخدام البيانات السرية confidential data تعطل في وظائف النظام الالكتروني Malfunction in electronic system وبالتالي خسارة عوائد الشركة أو الصناعة.

كما ركزت دراستي (Manoj 2021; Asakpa,2023) الى وجود تأثيرات اقتصادية وتنظيمية وعلى سمعة الشركة نتيجة اختراقات الأمن السيبراني، فالنسبة للأثار الاقتصادية تتمثل في سرقة الملكية الفكرية الخاصة بالشركة ومعلومات الشركة وتوقف عملياتها وتكاليف إصلاح النظم المخترقة، وبالنسبة للآثار على سمعة الشركة تتضح في تكاليف خسارة ثقة العملاء وخسارة العملاء الحاليين والمستقبليين لصالح المنافسين، وبالنسبة للآثار القانونية فقد تعاني الشركة من غرامات أو عقوبات قانونية نتيجة الجرائم والاختراقات السيبرانية.

وفي نفس السياق، ركزت دراسات اخري (Cheng et al. 2022; Sari et al.2024; Aboukari et al.2024) على أثر الاختراقات السيبرانية لأنشطة المؤسسات المالية عند تقديمها للخدمات على الخفض من الثقة في تلك المؤسسات، واتلاف البيانات الاساسية للمؤسسات، ووجود آثار اقتصادية وتنظيمية جوهرية على الشركات التي تعرضت لاختراقات سيبرانية مثل سرقة

معلومات الشركة وتوقف عملياتها وتكاليف اصلاح النظم المخترقة، وتكاليف خسارة ثقة العملاء وخسارة العملاء الحاليين والمستقبليين لصالح المنافسين، ووجود أثار قانونية مثل وجود غرامات أو عقوبات قانونية نتيجة الجرائم والاختراقات السيبرانية، بما يؤثر على تخفيض ثروة حملة الأسهم لتلك الشركات. كما أوضح Fotis (2024) أن الاختراقات السيبرانية لها أثار اقتصادية جوهرية على تخفيض ثروة حملة الأسهم عند الافصاح عن تلك الاختراقات.

وبشأن **المردود الاقتصادي للإفصاح عن الاختراقات السيبرانية**، أوضحت (Chen et al. 2022; Ashraf et al. 2022; Jiang et al. 2023) وجود استجابة سلبية من جانب المستثمرين عند التأخر في الافصاح عن الاختراقات السيبرانية، وتزداد الاستجابة السلبية للإفصاح عن الاختراقات السيبرانية بصورة جوهرية مع انخفاض مستوي الإفصاح عن الاختراقات السيبرانية بصرف النظر عن شدة الاختراقات السيبرانية، ولكن تنخفض الاستجابة السلبية للمستثمرين في حالة القيام بإفصاح تفصيلي عن الاختراقات السيبرانية، بما يوضح أهمية دور الإفصاح التفصيلي في الوقت المناسب عن الاختراقات السيبرانية لتخفيض الأثر السلبي للاختراقات على قيمة الاستثمار في الشركة.

٢/٦- الأمن السيبراني، وإدارة مخاطر الأمن السيبراني والإفصاح عنها: المفهوم والمردود الاقتصادي

اهتمت الدراسات المحاسبية (Von Solms and Van Niekerk 2013; Santhosh and Thiyagu 2022) بالتركيز على مفهوم الأمن السيبراني واختراقات الأمن السيبراني وإدارة مخاطر الأمن السيبراني

فعرفت دراسة Von Solms and Van Niekerk (2013) الأمن السيبراني بأنه حماية الفضاء الالكتروني والمعلومات والبنية التحتية لتكنولوجيا المعلومات التي تدعم الفضاء السيبراني، ومستخدمي الفضاء السيبراني وقدرات هؤلاء المستخدمين، والتي تتضمن القدرات الملموسة وغير الملموسة المعرضة للهجوم والاختراق السيبراني.

كما عرفت دراسة Santhosh and Thiyagu (2022) الأمن السيبراني بأنه مجموعة من الإجراءات الأمنية – ضمن اجراءات أمن المعلومات – بهدف حماية الفضاء الالكتروني (الشبكات

وأنظمة تقنية المعلومات والأجهزة وبرامج وأصول الشركة) من الوصول والتعرض لمخاطر الهجمات السيبرانية.

كما أضافت دراسة Li and Liu (2021) بأن الأمن السيبراني هي إجراءات ومقاييس عملية لحماية المعلومات والشبكات والبيانات من مخاطر الاختراق السيبراني الداخلية والخارجية، بحيث يضمن للأفراد المصرح لهم بالوصول لتلك المعلومات.

وفي نفس السياق عرفت دراسة Manoj (2021) الأمن السيبراني بأنها العمليات والتكنولوجيات المصممة لحماية الشبكات والحاسبات والبيانات من الدخول غير المصرح به وسرقة البيانات وأتلاف النظم المرتبطة بالإنترنت من خلال مخترقي الشبكات Hackers.

وبالتالي يمكن للباحث تعريف الأمن السيبراني بأنه: **مجموعة من الاجراءات والمقاييس الأمنية بهدف حماية الفضاء الالكتروني (الشبكات وأنظمة تقنية المعلومات والأجهزة والبرامج الخاصة بالشركات)، بحيث يضمن للأفراد المصرح لهم بالوصول لتلك المعلومات، ويمنع اختراقات أو سرقة واتلاف البيانات أو انظمة الشركات**".

وبشأن إدارة مخاطر الأمن السيبرانيCybersecurity risk management، عرفت AICPA (2017a) إدارة المخاطر السيبرانية بأنها قيام الشركة بمجموعة من السياسات والعمليات والضوابط لحماية الأنظمة والمعلومات من الحوادث السيبرانية التي يمكن أن تهدد أهداف الأمن السيبراني للشركة، والحوادث السيبرانية التي لم يتم منعها أو اكتشافها أو الاستجابة لها وتخفيضها في الوقت المناسب. كما قدم AICPA (2017a) إطار إدارة مخاطر الأمن السيبراني يشمل **ثلاثة مكونات** هي؛ وصف برنامج إدارة مخاطر الأمن السيبراني، ووجود توافق مع معايير البرامج وتأكيدات الإدارة حول فعالية إجراءات الأمن السيبراني، ورأي مراقب الحسابات عن افصاحات الإدارة وفعالية إجراءات الأمن السيبراني. ويتضمن الإطار مجموعتين من المعايير أولهما **معايير الوصف** الخاصة بإدارة مخاطر الأمن السيبراني، **ومعايير الرقابة** لمتابعة وتقييم اجراءات الأمن السيبراني.

كما عرفت دراسة Alina et al. (2017) إدارة المخاطر السيبرانية بانها الأنشطة التي تساعد على حماية الموارد التكنولوجية وشبكات الشركة وبما يخفض من خسائر الاختراقات السيبرانية، وبما يؤدي لاستعادة النظم وعدم تعطيل عمليات التشغيل بالشركات. كما عرفت دراسة Melaku

(2023) إدارة المخاطر السيبرانية بأنه الأنشطة التي تهدف لاكتشاف التهديدات ونقاط الضعف الأمنية للمؤسسات بهدف معالجة مخاطر الأمن السيبراني بالشركة.

وبناء على ما سبق يمكن للباحث تعريف **إدارة مخاطر الأمن السيبراني** بأنها: السياسات والانشطة التي تهدف **لتحديد الاختراقات السيبرانية** نتيجة نقاط الضعف في الموارد المرتبطة بأنظمة المعلومات والاتصال بالشركة، **وتنفيذ اجراءات وضوابط أمن سيبراني فعالة** للتخفيف من الأثار السلبية لهذه الاختراقات، **والتقييم الدوري للمخاطر السيبرانية**، ولإدارة مخاطر الأمن السيبراني ذاتها.

وبالنسبة **للإفصاح عن إدارة مخاطر الأمن السيبراني**، أوضحت دراسة Berkman, et al. (2018) بأنه التقرير عن معلومات تساعد أصحاب المصالح المختلفة في الشركة في تقييم منهجية إدارة مخاطر الأمن السيبراني بالشركة، والقرارات التي يتخذها مجلس الإدارة لتخفيض تلك المخاطر.

كما أوضحت دراسة على وعلي (٢٠٢٢) اتجاه العديد من الهيئات والمنظمات المهنية في معظم دول العالم لإصدار إرشادات للإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني لمساعدة أصحاب المصالح في تقييم أداء الشركة في إدارة مخاطر الأمن السيبراني. وركزت الدراسة على التقرير الذي سوف تعده الشركات للإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني، ويتكون من ثلاثة اقسام وفق (AICPA,SOC, 2017b):

القسم الأول: وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني بالاستعانة بمعايير وصف برنامج إدارة مخاطر الأمن السيبراني وفق (2017a) AICPA.

القسم الثاني: تأكيدات الإدارة بأن إعداد ووصف التقرير يتم وفق معايير الوصف، كما تؤكد إدارة الشركة على فعالية ضوابط الرقابة على برنامج إدارة مخاطر الأمن السيبراني وفق معايير خدمات الثقة.

القسم الثالث: رأي مراقب الحسابات عن فحص ومراجعة تقرير الشركة عن إدارة المخاطر السيبرانية، وذلك مع استخدام مراقب الحسابات معايير الوصف والرقابة المحددة من قبل AICPA لكي يتمكن من تقييم الضوابط الرقابية داخل برنامج إدارة مخاطر الأمن السيبراني، وفعالية عمل تلك الضوابط للحفاظ على سرية وسلامة وتوافر المعلومات، ومن ثم الحصول على أدلة اثبات كافية ومناسبة لتقديم أساس معقول لرأيه عن تقرير إدارة مخاطر الأمن السيبراني.

وأصدرت SEC (2022) تعديلاً بشأن متطلبات الإفصاح الخاصة بإدارة مخاطر الأمن السيبراني يتضمن الافصاح عن مخاطر الأمن السيبراني الفردية التي تشكل في مجملها أحداثاً هامة، وإعداد تقرير سنوي عن خبرة مجلس الإدارة في مجال الأمن السيبراني والسياسات المتبعة لمواجهة مخاطر الأمن السيبراني والإفصاح الدوري عن سياسات إدارة مخاطر الأمن السيبراني. كما اضافت دراسة Smaili, and Khalili (2023) أهمية الإفصاح عن تنفيذ سياسات وأنشطة إدارة المخاطر السيبرانية الملائمة التي تخفض من تكاليف الهجمات السيبرانية.

وبناء على ما سبق يمكن تعريف الإفصاح عن إدارة مخاطر الأمن السيبراني بأنه " تقرير تعده الشركات للإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني ويتكون من ثلاثة أقسام وهي؛ **وصف الإدارة** لبرنامج إدارة مخاطر الأمن السيبراني بالاستعانة بمعايير وصف برنامج إدارة مخاطر الأمن السيبراني، **و تأكيدات الإدارة** بأن التقرير يتم وفق معايير الوصف ووفق معايير خدمات الثقة، **ورأي مراقب الحسابات** عن فحص ومراجعة تقرير الشركة عن إدارة المخاطر السيبرانية، والقرارات التي يتخذها مجلس الإدارة لتخفيض تلك المخاطر، بالإضافة إلى **التقرير السنوي عن خبرة مجلس الإدارة** في مجال الأمن السيبراني و **السياسات** المتبعة لمواجهة مخاطر الأمن السيبراني والإفصاح الدوري عن سياسات إدارة مخاطر الأمن السيبراني" .

ويمكن للشركات استخدام إطار تقرير إدارة مخاطر الأمن السيبراني الذي قدمه(AICPA,SOC(2017b للإفصاح عن هذا التقرير ضمن القوائم المالية للشركة أو في تقرير مجلس الإدارة (ضمن مرفقات القوائم المالية).

وبشأن الوضع في مصر، فقد تم وضع الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١) من جانب المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء وبرئاسة وزير الاتصالات وتكنولوجيا المعلومات. ويمثل الهدف الاستراتيجي لهذا المجلس مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية التحتية للاتصالات وتكنولوجيا المعلومات وتطبيقاتها وتوفير البيئة الامنة للقطاعات لتقديم الخدمات الالكترونية المتكاملة. وتشمل الاستراتيجية كل من تعريف التحديات والمخاطر السيبرانية والتي تتمثل في خطر اختراق وتخريب البنية التحتية للاتصالات وتكنولوجيا المعلومات ومخاطر الحرب السيبرانية ومخاطر سرقة الهوية والبيانات الخاصة. وركزت الاستراتيجية على تحديد أهم القطاعات الحيوية المستهدفة وتشمل قطاع الاتصالات وتكنولوجيا

المعلومات، قطاع الخدمات المالية، وقطاع الطاقة، وقطاع الخدمات الحكومية وقطاع النقل، والمواصلات، وقطاع الاعلام، والثقافة.

وبشأن المردود الاقتصادي للإفصاح عن إدارة المخاطر السيبرانية، أشارت دراسة (Jiang et al.2022 ;٢٠٢٤،كعموش) إن الإفصاح عن إدارة مخاطر الأمن السيبراني يقدم إشارات للمستثمرين لاتخاذ القرارات الاستثمارية في أسهم الشركات نتيجة تأثيرها في تقييم مخاطر الأسهم وزيادة الثقة المتبادلة بين الشركة واصحاب المصالح من خلال توفير المعلومات التي تساعد أصحاب المصالح في تقييم الخسائر الحالية والمستقبلية الناتجة عن حدوث الاختراقات السيبرانية. كما اوضحت دراسة Kelton and Pennington (2020) إن الافصاح المسبق عن إدارة مخاطر الأمن السيبراني يّمكن من التنبؤ بأثار الاختراقات السيبرانية وبالتالي يحد من أثارها السلبية المتوقعة على سمعة الشركة وثروة المساهمين. كما أوضحت دراسة Kelton (2021) أن الإفصاح المسبق عن إدارة المخاطر السيبرانية يحقق مصالح إيجابية للمديرين من خلال تجنب الأثار السلبية على سمعة الإدارة نتيجة اختراق البيانات.

كما أضافت دراسة Klemash et al. (2020) أن الإفصاح عن إدارة مخاطر الأمن السيبراني يبني الثقة لدى أصحاب المصالح عن كيفية قيام مجلس الإدارة بمسئولياته لإدارة مخاطر الأمن السيبراني والرقابة عليها، وزيادة جاذبية الاستثمار في الشركة التي تقوم بالإفصاح عن إدارة المخاطر السيبرانية بالمقارنة بالشركات التي لا تقوم بالإفصاح بصورة مناسبة. بينما أوضح شرف (٢٠٢٣) أن افصاح الشركة عن إدارة المخاطر السيبرانية قد يضر بمصالح الإدارة نتيجة الكشف عن خطط الأمن السيبراني بالشركة، والتي قد يستغلها المهاجمون لتحقيق اختراقات سيبرانية في المستقبل، بالرغم من أثارها الايجابية على المستثمرين غير المحترفين في تلك الشركات.

٦ / ٣-تحليل الدراسات المحاسبية الخاصة بالعلاقة بين الاختراقات السيبرانية والافصاح عنها وقرار الاستثمار في الشركات

اهتمت الدراسات المحاسبية (Tweneboah -Kouda et al,2018; Cheng et al. 2022; Aboukari et al.2024) بتحليل العلاقة بين اختراقات الأمن السيبراني والإفصاح عنها والاستثمار في الشركات التي تعرضت للاختراقات السيبرانية.

فقد هدفت دراسة(2018) .Tweneboah –Kouda et al إلى تحليل تأثير إعلانات الهجمات الإلكترونية على أسعار أسهم لـ ٩٦ شركة مدرجة في مؤشر S&P 500 خلال الفترة من ٣ يناير التي٢٠١٣ إلى ٢٩ ديسمبر ٢٠١٧.

وتم إجراء التحليل الاحصائي زمنيا وعلى مستوى الصناعة، مع تحليل سلاسل العوائد، والتقلبات في تلك العوائد.

وأشارت نتائج الدراسة إلى اختلاف جوهرية الآثار التراكمية للهجمات الإلكترونية على أسعار الشركات المدرجة دون تقسيمها إلى القطاعات المختلفة؛ حيث تستجيب شركات القطاع المالي بصورة تراكمية للهجمات الإلكترونية خلال فترة ثلاثة أيام مقارنة بالقطاعات الأخرى؛ بينما تكون شركات التكنولوجيا أقل استجابةً للإفصاح عن الهجمات السيبرانية، حيث قد تمتلك هذه الشركات الأدوات والتقنيات اللازمة للتعامل مع الهجمات الإلكترونية واسعة النطاق.

كما أوضحت نتائج الدراسة أن هناك استجابة تراكمية للشركة تجاه الهجمات الإلكترونية لمدة أطول في قطاع البيع بالتجزئة، بينما لا توجد استجابة تراكمية للشركة تجاه الهجمات الإلكترونية لكل من القطاعات الصناعية وتكنولوجيا المعلومات والصحة. كما أشارت نتائج الدراسة إلى وجود دليل معنوي على استجابة تراكمية تجاه الهجمات الإلكترونية للصناعات المالية وتقل هذه الاستجابة خلال الفترة طويلة الأجل. وتميل شركات القطاع المالي إلى الاستجابة تراكميًا للهجمات الإلكترونية خلال فترة ثلاثة أيام مقارنة بالقطاعات الأخرى، وتميل شركات التكنولوجيا إلى أن تكون أقل استجابةً لإعلان الهجمات السيبرانية، ومن المحتمل أن تمتلك هذه الشركات الأدوات والتقنيات اللازمة للتعامل مع الهجمات الإلكترونية واسعة النطاق.

كما هدفت دراسة (2020) .Gao et al إلى تحليل محتوى وخصائص الافصاح عن مخاطر الاختراقات السيبرانية للشركات المساهمة، والعوامل المحددة لاتجاهات الإفصاح عن تلك المخاطر.

وتم اختيار عينة من افصاحات الشركات عن مخاطر الأمن السيبراني من عام ٢٠١١ حتى عام ٢٠١٨ ضمن تقرير 10–K بناء على قانون (Public Law 111–274,2010) والذي نص على افصاح الشركات على المخاطر القضائية المؤثرة على تقييم الشركات لمخاطر الأمن السيبراني. وعلى الرغم من أهمية مخاطر الأمن السيبراني وتأثيرها بدرجة جوهرية على العمليات التجارية وسلامة افصاحات الشركات، إلا أن هناك أبحاثًا تجريبية محدودة حول اتجاهات وممارسات الإفصاح عن مخاطر الاختراقات السيبراني للشركات المساهمة.

وأظهرت نتائج الدراسة أن مخاطر الاختراقات السيبرانية الأكثر إفصاحاً هي مخاطر تعطيل الخدمة/العمليات، ومخاطر اختراق البيانات. كما اتضح زيادة الإفصاح عن مخاطر الأمن السيبراني خلال فترة الدراسة. وترتبط هذا الزيادة بإصدار توجيهات لجنة الأوراق المالية والبورصة الأمريكية لعامي ٢٠١١ و٢٠١٨. وأشارت نتائج الدراسة إلى أن الإفصاحات عن مخاطر الاختراقات السيبرانية تعتبر أكثر صعوبة في القراءة مع زيادة حجم الشركة، وأسهل في قابليتها للقراءة مع زيادة نسبة الأصول غير الملموسة أو بعد تغيير للمديرين التنفيذيين.

كما أشارت دراسة Jiang et al. (2022) إلى أن تكرار الاختراقات السيبرانية للشركة واستجابة السوق لتلك الاختراقات والإفصاح عنها يؤثر على سلوك الإفصاح عن المخاطر السيبرانية لتلك الشركات. وأشارت نتائج الدراسة الي وجود استجابة سلبية لسوق الأوراق المالية نتيجة تلك الاختراقات، بما يدفع الشركات الي الكشف عن تفاصيل إضافية للتخفيف من الاستجابة السلبية لتلك الاختراقات. كما اتضح أن الشركات التي تتصف بارتفاع المخاطر والاختراقات السيبرانية (مثل الشركات التي تنتمي للقطاع المالي) تقدم مستوى أعلى من الإفصاحات بالمقارنة بالشركات في الصناعات الأقل مخاطر سيبرانية.

كما هدفت دراسة D'Arcy and Basoglu (2022) الى تحليل دور الضغوط الاجتماعية والمؤسسية لزيادة افصاح الشركات عن حوادث الاختراق السيبراني، وتأثر مصدر الاختراق الداخلي أو الخارجي مع نوع الضغوط والافصاح عنها في التقارير السنوية أو ربع السنوية في الشركات المقيدة في البورصة الأمريكية.

وأشارت نتائج الدراسة إلى تأثر افصاحات الشركات عن الاختراقات السيبرانية بالضغوط العامة بصورة أكثر حدة الناتجة عن اختراقات البيانات خاصة بالنسبة للاختراقات السيبرانية الخارجية بالمقارنة بالاختراقات السيبرانية الداخلية. وتدعم نتائج الدراسة أهمية الضغوط الاجتماعية والمؤسسية نتيجة مصادر الاختراقات السيبرانية، وأثرها على العوامل التي تدعم الإفصاحات المناسبة عن الاختراقات السيبرانية.

كما هدفت دراسة Ashraf et al. (2022) الي مناقشة أثر الافصاح عن الاختراقات السيبرانية بعد حدوثها مع وجود إلزام من هيئة الأوراق المالية الأمريكية للإفصاح عن تلك الاختراقات السيبرانية خلال أربعة ايام.

تم اختيار عينة من ٢٤٠ اختراق سيبراني من عام ٢٠١٠ حتى عام ٢٠٢٠ لشركات مسجلة في البورصات الأمريكية. وبتحليل الاختلافات في الإفصاحات عن الاختراقات السيبرانية، أشارت نتائج الدراسة إلى وجود افصاحات الزامية بنسبة ٩٠% أسرع في الشركات التي قامت بالالتزام بالإفصاح عن الاختراقات مع وجود نسبة ٥٨% من الشركات أفصحت بصورة أقل تفصيلاً. كما اتضح وجود استجابة سلبية من جانب المستثمرين عند التأخر في الافصاح عن الاختراقات السيبرانية، ولكن تنخفض الاستجابة السلبية في حالة القيام بإفصاح تفصيلي عن الاختراقات السيبرانية، بما يوضح وجود مفاضلة بين الإفصاحات الالزامية عن الاختراقات السيبرانية، والإفصاحات التفصيلية عن تلك الاختراقات.

كما هدفت دراسة De Arroyabea and De Arroyabe (2023) الى تحليل أثر اختراقات الأمن السيبراني على الشركات الصغيرة ومتوسطة الحجم، مع الأخذ في الاعتبار دور الأمن السيبراني في تلك الشركات.

وتم القيام بدراسة ميدانية لـ ١٣٤٨ صغيرة ومتوسطة الحجم في المملكة المتحدة من أكتوبر ٢٠١٦ حتى يناير ٢٠١٧ بهدف مسح الاختراقات السيبرانية في تلك الشركات ودرجة شدة الاختراقات والآثار الاقتصادية والمالية على تلك الشركات.

وأشارت نتائج الدراسات إلى أن الشركات الصغيرة والمتوسطة الحجم تخضع لمجموعة واسعة من الهجمات مثل الاختراقات الناتجة عن هجمات الهندسة الاجتماعية، والتصيد الاحتيالي، والهجمات الآلية، وبرامج الفدية بهدف اختطاف المعلومات، والهجمات غير الآلية، والبرامج الضارة التي تهدف إلى اختراق شبكة الشركة، أو الاختراقات الناتجة عن الاستخدام غير السليم لأصول الشركة، وبذلك فإن الشركات الصغيرة والمتوسطة الحجم معرضة لهجمات القراصنة. بدرجة كبيرة مع نقص توافر أدوات الأمن السيبراني لتلك الشركات. كما اتضح أن أكثر الاختراقات لتلك الشركات هو استلام الموظفين لبريد إلكتروني احتيالي أو توجيههم إلى مواقع احتيالية، خاصة بأشخاص أو شركات وهمية، واختراق أجهزة الحاسب بفيروسات أو برامج تجسس أو برامج ضارة أخرى. كما أوضحت نتائج الدراسة شدة تأثير الاختراقات في الشركات صغيرة ومتوسطة الحجم على قيمة تلك الشركات، خاصة مع ضعف إجراءات الأمن السيبراني في تلك الشركات.

كما هدفت دراسة Demk and Kaplan (2023) إلي تحليل اسباب اختراقات الأمن السيبراني ودور استراتيجيات الأمن السيبراني في تقليل احتمال حدوث الاختراقات السيبرانية. وتم

استخدام تجربة ٢ × ٢ بين المشاركين، لتحديد مدى اكتشاف استراتيجيات إدارة مخاطر الأمن السيبراني للاختراقات ودور الرئيس التنفيذي في الإفصاح عن مخاطر الأمن السيبراني، وكان المشاركون ١٠٨ مستثمر من غير المحترفين ٦٩ من الذكور، و ٣٩ من الإناث.

وأوضحت نتائج الدراسة أن افصاح الشركات عن اختراقات الأمن السيبراني لا تقضي على خطر الاختراقات. كما أظهرت نتائج الدراسة أن وجود اعتذار من الرئيس التنفيذي عن الاختراقات السيبرانية يؤثر بشكل إيجابي على انطباع المستثمرين عن الاستثمار وإدراكهم للثقة بالرئيس التنفيذي للشركة، ومع ذلك، فإن اعتذار الرئيس التنفيذي لا يؤثر بشكل كبير على قرار الاستثمار بالشركة.

وفي نفس السياق، هدفت دراسة Chen et al. (2023) الي تحليل قرارات المديرين للإفصاح عن العوامل المرتبطة بمخاطر الأمن السيبراني بعد حدوث الاختراقات السيبرانية وفق شدة اختراقات الأمن السيبراني. وتم استخدام عينة من الشركات التي تعرضت لاختراقات الأمن السيبراني بالمقارنة مع الشركات التي لم تتعرض لاختراقات البيانات.

وأشارت نتائج الدراسة إلى زيادة الإفصاحات عن العوامل المرتبطة بالاختراقات السيبرانية، واتضح وجود استجابة سالبة بصورة جوهرية عند تقليل الإفصاح عن عوامل مخاطر الأمن السيبراني بصرف النظر عن شدة الاختراقات، بما يوضح توقع سوق الأوراق المالية زيادة الإفصاح بعد حدوث اختراقات البيانات.

كما هدفت دراسة Aboukari et al.(2024) الى تحليل واختبار العلاقة بين إفصاحات الشركة عن الاختراقات السيبرانية واحتمال تكرار الاختراقات السيبرانية بالشركات. وتم استخدام ٢٩٣ اختراق سيبراني لـ ٥٠٧٥ شركة مسجلة في البورصات الأمريكية من عام ٢٠٠٥ حتى عام ٢٠١٨. وأشارت نتائج الدراسة أنه كلما زادت الإفصاحات الإيجابية Positive tone في التقارير المالية السنوية، كلما ازدادت الاختراقات السيبرانية للشركة، حيث كلما افصحت الشركة عن خصائص إيجابية مثل وجود تدفقات نقدية إيجابية هامه أو ارتفاع معدل ربحية السهم، كلما صارت هدف أكثر جاذبية للاختراقات السيبرانية. كما أشارت نتائج الدراسة إلى أهمية تحليل قنوات الاتصال غير التقليدية مثل وسائل التواصل الاجتماعية والمنصات المالية غير التقليدية لاستكشاف أثار الافصاح عن الاختراقات السيبرانية في تلك الوسائل على قرارات المستثمرين بالشركات. كما اتضح أن

انخفاض القابلية للقراءة للإفصاح عن الاختراقات السيبرانية، كلما زاد احتمال الاختراقات السيبرانية، وذلك مع الأخذ في الاعتبار أثر الصناعة واختلاف السنوات في الدراسة.

كما هدفت دراسة Sari et al. (2024) إلى تحليل أهمية قرارات الإفصاح عن العوامل المؤثرة على مخاطر الأمن السيبراني بسبب العدد الكبير من اختراقات البيانات التي تحدث على مدار العام. كما تم إجراء مراجعة الدراسات السابقة لتحديد على العوامل المؤثرة على الإفصاح عن مخاطر الأمن السيبراني.

وأظهرت نتائج الدراسة أهمية كل من مستوي اختراق الأمن السيبراني وحوادث الاختراق السيبراني السابقة، والعمل عن بعد، وحجم مجلس الإدارة، واستقلالية مجلس الإدارة، وتنوع الجنس في مجلس الإدارة، والمساهمين الأجانب، والأصول غير الملموسة، وحجم الشركة، ونمو الشركة، ومستوى الرفع المالي بالشركة، وربحية الشركة، ولجنة التكنولوجيا بالشركة، والتغيير للمديرين التنفيذيين، كعوامل مؤثرة على الإفصاح عن مخاطر الأمن السيبراني.

ويخلص الباحث من تحليل الدراسات السابقة ذات العلاقة باختراقات السيبرانية والإفصاح عنها، والاستثمار في الشركات إلى إمكانية وجود استجابة سلبية للاختراقات السيبرانية خاصة مع تكرار تلك الاختراقات على قرار الاستثمار بالشركات، بالإضافة إلى اختلاف هذه الاستجابة وفقاً للقطاع الي تنتمي له الشركة التي تم اختراقها ونوع الاختراق السيبراني ونوع الإفصاح عن تلك الاختراقات، وبالتالي يمكن صياغة **فرضي البحث الأول والثاني كما يلي:**

الفرض الأول:

H1: تؤثر اختراقات الأمن السيبراني بصورة سلبية معنوية على الاستثمار بالشركات المصرية

H1a: تؤثر اختراقات الأمن السيبراني بصورة سلبية معنوية على قرار الاستثمار بالشركات المصرية

H1b: تؤثر اختراقات الأمن السيبراني بصورة سلبية معنوية على قيمة الاستثمار بالشركات المصرية

الفرض الثاني:

H2: يؤثر الافصاح عن اختراقات الأمن السيبراني بصورة سلبية معنوية على الاستثمار بالشركات المصرية

H2a: يؤثر الافصاح عن اختراقات الأمن السيبراني بصورة سلبية معنوية على قرار الاستثمار بالشركات المصرية

H2b: يؤثر الافصاح عن اختراقات الأمن السيبراني بصورة سلبية معنوية على قيمة الاستثمار بالشركات المصرية

٦/ ٤- الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والإفصاح عنها وقرار الاستثمار في الشركات:

اهتمت الدراسات المحاسبية (Lee 2021; Ramírez et al. 2022; Huang and Murthy 2024) بأثر الإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين اختراقات الأمن السيبراني والافصاح عنها وقرار الاستثمار في الشركات.

فقد هدفت دراسة Yang et al. (2020) إلى اختبار إدراك المستثمرين عن منافع إطار التقرير عن إدارة المخاطر السيبرانية الذي قدمته جمعية المحاسبين القانونيين الأمريكية من خلال تحليل الإفصاحات عن الشركات الأمريكية المسجلة في قاعدة Amazon's Mechanical Turk platform. وأشارت نتائج الدراسة الي وجود علاقة ايجابية بين منافع المستثمرين من الإفصاح عن إدارة مخاطر الأمن السيبراني وقرار المستثمرين بالاستثمار في الشركات التي تفصح عن إدارة مخاطر الأمن السيبراني. كما ترتبط جودة المعلومات المحاسبية والوعي بمخاطر الأمن السيبراني بصورة ايجابية بالمنافع المدركة من إطار إدارة مخاطر الأمن السيبرانية، وقرار الاستثمار في تلك الشركات.

كما هدفت دراسة الزيود (٢٠٢٠) إلى تحليل جوانب إدارة المخاطر السيبرانية وأنواعها ومجالاتها وأدوات إدارة وتقييم المخاطر في البنوك الأردنية، بهدف الحفاظ على سلامة البنوك ومركزها المالي والحفاظ على أمن المعلومات والشبكات.

وأشارت نتائج الدراسة إلى التزام البنوك الأردنية بالسياسات الخاصة بأمن المعلومات والأمن السيبراني، مع الأخذ في الاعتبار منهجيات وإجراءات إدارة مخاطر الأمن السيبراني، وتنفيذ إجراءات تقييم مخاطر الأمن السيبراني بشكل دوري وتحديثها وتوثيقها وفق جدول زمني. كما تقوم البنوك الأردنية بنشر دليل الحوكمة المؤسسية لتكنولوجيا المعلومات ضمن التقارير السنوية أو ضمن تقارير خاصة على مواقع البنوك الأردنية. وأوصت الدراسة بتوضيح سياسات الأمن السيبراني بشكل أدق، ونشر مزيد من الإيضاحات في التقارير السنوية بخصوص التهديدات والاختراقات السيبرانية وقدرة البنوك على معالجتها.

كما هدفت دراسة (2021) Lee إلى تحليل أهمية دور الأمن السيبراني في إدارة مخاطر المنشآت، حيث يؤدي التحسن في اجراءات الأمن السيبراني إلى زيادة مستوى ثقة العملاء بالشركة، وزيادة ربحيتها، وحماية البيانات، مع أهمية دور تشريعات الخصوصية في فعاليه إجراءات إدارة الأمن السيبراني. وقدمت الدراسة إطاراً لإدارة الأمن السيبراني يتضمن أربعة طبقات و هي؛ **بيئة الأمن السيبراني** (ويشمل شركاء سلاسل الإمداد والعملاء والتشريعات المنظمة للأمن السيبراني و مقدمي تكنولوجيا ومستشاري الأمن السيبراني، ومخترقي الحاسبات)، **البنية التحتية للأمن السيبراني** (وتتضمن المنشآت والمستخدمين الداخليين و تكنولوجيا أمن الشبكات)، **وتقييم مخاطر الأمن السيبراني** (ويشمل تحديد المخاطر وقياسها وتحليل الاستثمار المطلوب لإدارة مخاطر الأمن السيبراني)، **أداء مخاطر الأمن السيبراني** (وتتضمن تنفيذ إجراءات الأمن السيبراني ومتابعة ورقابة إجراءات الأمن السيبراني و التحسين المستمر لتلك الاجراءات).

وأوضحت نتائج الدراسة صعوبة قياس منافع وتكاليف إدارة مخاطر الأمن السيبراني باعتبارها عائق للاستثمار في الشركات وفي تكنولوجيا الأمن السيبراني بالشركات. وأوضحت الدراسة أهمية دور إدارة الشركة في تحديد مدى الحاجة لاقتناء تكنولوجيا الأمن السيبراني الملائمة، وتحديد الأولويات التكنولوجية لتحسين إدارة مخاطر الأمن السيبراني، مع التركيز على التكنولوجيات التي تدعم حماية الأمن السيبراني.

كما أشارت الدراسة إلى أنه يمكن لإدارة الشركة تقليل آثار الجرائم السيبرانية وتعزيز القيمة الاقتصادية المستقبلية لتلك الشركات، بما يزيد من مستوى الثقة وفرص الأعمال مع العملاء، وذلك من خلال فهم وتقييم وتنفيذ طبقات إدارة مخاطر الأمن السيبراني لتحقيق إدارة شاملة لهذه المخاطر.

وأيضا أشارت الدراسة إلى أنه يمكن أن تؤدي اختراقات الأمن السيبراني إلى خسائر مالية، ضخمة ويساهم منع هذه الاختراقات من تقليل تلك الخسائر، نظرًا لأن الاستثمار في تقنيات الأمان يعد نفقات رأسمالية، فمن المحتمل أن يخضع هذا الاستثمار لمراجعة الإدارة العليا للموافقة على الميزانية. ويتحقق الاستثمار الأمثل عند النقطة التي تتساوى فيها الزيادة الحدية في تكلفة الاستثمار في الأمن السيبراني مع النقص الحدي في الخسارة المالية. ويساعد التحسين المستمر الشركات على التكيف بشكل صحيح مع التغيرات السريعة في النظام البيئي السيبراني لتكون أكثر استعدادًا لمواجهة التهديدات السيبرانية، وذلك بالإضافة إلى متابعة اتجاهات الأمن السيبراني على مستوى الصناعة. ويعتمد قرار الاستثمار السيبراني على تقليل تكاليف الأمن السيبراني، مع دمج الأساليب المالية

التقليدية مثل NPV وROI وطرق استرداد الأموال في عملية اتخاذ القرار الاستثماري في إدارة الأمن السيبراني. وتعتبر إدارة المخاطر السيبرانية جزء من إدارة المخاطر الشاملة للشركة والتي تشمل أيضًا قضايا المخاطر التنظيمية غير السيبرانية.

وفي نفس السياق، اهتمت دراسة Jeyarai et al. (2021) باختبار العلاقة بين تهديدات الأمن السيبراني واستجابة إدارة مخاطر الأمن السيبراني. وصنفت الدراسة التهديدات السيبرانية إلى أربعة أنواع وهي تهديدات مادية، وتهديدات للأفراد، وتهديدات للاتصالات والبيانات، وتهديدات تشغيلية، وتم فحص استجابات الشركات لهذه التهديدات.

وتم تحليل استجابات ٨٧ شركة لتهديدات الأمن السيبراني وتقييم هذه التهديدات. وأظهرت نتائج الدراسة وجود أثار سلبية للتهديدات السيبرانية، ووجود تأثير لاستجابة إدارة المخاطر السيبرانية خاصة بالنسبة للتهديدات المادية والتشغيلية (وفق الاستجابة التقنية)، والتهديدات التشغيلية والاتصالات) الاستجابة غير التقنية) ، وتهديدات الأفراد على الاستجابة الشاملة لإدارة المخاطر، بما يؤثر على تخفيض الاستجابات السلبية للتهديدات السيبرانية.

كما هدفت دراسة Chen et al. (2022) تحليل أثر افصاح الإدارة عن إدارة مخاطر الأمن السيبراني على حدة الاختراقات السيبرانية. وتم تحليل موقفين للمديرين من الجانب الاقتصادي وفق مستوى الخطر الأمثل للشركة ومن الجانب الأخلاقي وفق نظرية أصحاب المصالح بالشركة، وتم استخدام عينة من٢٧٩ شركة واجهت اختراقات سيبرانية من عام ٢٠٠٥ حتى عام ٢٠١٨. وتم تسجيل تلك الاختراقات من خلال مؤسسة Privacy Rights Clearinghouse وسجلات SEC's EDGAR

وأشارت نتائج الدراسة أنه كلما زادت الاختراقات السيبرانية لبيانات الشركات، كلما زاد مقدار الإفصاح عن إدارة مخاطر الأمن السيبراني والعوامل المؤثرة بها، وذلك بالمقارنة بالشركات التي لم تعاني من اختراقات سيبرانية لأنظمتها. كما اتضح أن عدم وجود افصاحات عن مخاطر الأمن السيبراني يؤدي إلى أثر سلبي معنوي على أسعار أسهم الشركات التي لم تقم بالإفصاح عن الاختراقات السيبرانية، حتى إذا قامت الشركة بتخفيض مستوى المخاطر السيبرانية الخاصة بالشركة، من خلال زيادة الإفصاحات بعد الاختراقات السيبرانية.

كما هدفت دراسة Cheng et al. (2022) إلى تحليل تأثير الإفصاحات المختلفة عن إجراءات الأمن السيبراني على قرارات الاستثمار قبل وبعد أن يتم الإفصاح عن الاختراقات السيبرانية. وتم استخدام دراسة تجريبية لثلاث حالات قرار مختلفة وهي حالة عدم الإفصاح عن اجراءات الأمن السيبراني، وحالة التقرير عن إدارة المخاطر السيبرانية(CSRM) ، وحالة التقرير عن إدارة المخاطر السيبرانية CRSMمع تقرير مراجع داخلي، وأثر تلك الحالات على أحكام وقرارات الاستثمار في الشركات.

وأشارت نتائج الدراسة أنه عندما لا يوجد افصاح عن الاختراقات الأمنية، فإن قرارات المستثمرين لا تختلف في حالات القرار المختلفة، بما في ذلك عدم الإفصاح عن اجراءات الأمن السيبراني، وتقرير إدارة المخاطر السيبرانية(CSRM) ، وتقرير CSRM مع تقرير مراجع مستقل(IA) للتوكيد عن الإفصاحات عن الأمن السيبراني.

وأشارت نتائج الدراسة إلى استخدام المستثمرين غير المحترفين للتقارير المالية للشركات بشكل أساسي لاتخاذ قرارات الاستثمار، وذلك عندما لا توجد افصاحات سلبية خاصة بالاختراقات السيبرانية. كما أوضحت نتائج الدراسة أن المستثمرين غير المحترفين أقل استعدادًا للاستثمار في الشركة بعد معرفتهم بأن الشركة قد تأثرت بالاختراقات السيبرانية. كما أشارت نتائج الدراسة إلى أن الإفصاح عن معلومات إضافية حول برامج إدارة مخاطر الأمن السيبراني مع وجود تقرير مراجع داخلي (للتوكيد على تقارير CSRM) لشركة تعرضت لاختراقات للأمن السيبراني، يؤدي إلى نتائج سلبية على قيمة الشركة، ولا يخفض من التأثير السلبي للاختراقات خاصة للمستثمرين غير المحترفين.

كما هدفت دراسة يوسف (٢٠٢٢) أُثر الإفصاح عن إدارة مخاطر الأمن السيبراني على قرارات الاستثمار في الشركات المصرية المسجلة في البورصة المصرية. استخدمت الدراسة المنهج الوصفي باستقصاء أراء عينة من مدراء ونواب مدراء إدارة المخاطر في عدد من الشركات تقدر نسبتها بـ ٢٥% من الشركات المقيدة في أكبر خمس قطاعات من حيث حجم سوق المال والتي بها إدارة للمخاطر، من خلال استقصاء واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة.

وأظهرت نتائج الدراسة أن عدم إفصاح الشركات المقيدة بالبورصة المصرية عن إدارة مخاطر الأمن السيبراني يؤدي إلى أثار سلبية على أسعار واحجام التداول. وأوصت الدراسة بإصدار

البورصة المصرية والهيئة العامة للرقابة المالية والبنك المركزي الضوابط والإرشادات اللازمة لدعم الإفصاح عن انشطة الأمن السيبراني، واختراقاته وبرامج إدارة مخاطر الأمن السيبراني بالشركات.

كما هدفت دراسة(2023) Mazzoccoli الي تحليل دور فعالية استراتيجيات إدارة مخاطر الأمن السيبراني في تخفيض أثار الاختراقات السيبرانية. وأوضحت نتائج الدراسة أن الاستثمار في استراتيجيات إدارة المخاطر السيبرانية يخفض من تكلفة الأثار المترتبة على حدوثها، وتكلفة التأمين ضد الاختراقات السيبرانية (باستخدام شركة متخصصة لإدارة مخاطر الأمن السيبراني).

كما أوضحت نتائج الدراسة أهمية التوازن بين الاستثمار في استراتيجيات إدارة مخاطر الأمن السيبراني مع تكلفة التأمين ضد تلك الاختراقات السيبرانية، فتكون كفاءة الاستثمار في تلك الاستراتيجيات أكثر إذا كانت أقل من تكلفة التأمين ضد مخاطر الاختراقات السيبرانية بحيث تحقق تلك الاستثمارات وفورات مالية للشركة. ويتطلب ذلك التقييم الدقيق لتكاليف البدائل الاستراتيجية لإدارة مخاطر الأمن السيبراني. وتقل كفاءة الاستثمار في استراتيجيات إدارة مخاطر الأمن السيبراني مع زيادة قدرة الشركة استخدام تكاليف التأمين ضد الاختراقات السيبرانية (من خلال شركة متخصصة للتأمين ضد الاختراقات السيبرانية).

وتمتاز هذه الدراسة بالأخذ في الاعتبار تحليل تكاليف القيام باستراتيجيات إدارة مخاطر الأمن السيبراني من جانب، والتأمين ضد اختراقات الأمن السيبراني من خلال استخدام شركة متخصصة للقيام بالتأمين ضد اختراقات الأمن السيبراني من جانب أخر، وذلك بهدف تخفيض مخاطر وتكاليف الاختراقات السيبرانية على أنظمة الشركة.

كما أشارت الدراسة الى استخدام شركات متخصصة للتأمين ضد مخاطر الاختراقات السيبرانية نتيجة ارتفاع تكلفة خسائر الشركات لمعالجة الهجمات السيبرانية بالمقارنة باستثمارات الشركات في استراتيجيات إدارة مخاطر الأمن السيبراني

كما هدفت دراسة (2024)Huang and Murthy إلى اختبار وتحليل التأثير المحتمل لإفصاح الإدارة عن استراتيجية إدارة المخاطر السيبرانية على المستثمرين غير المحترفين(نتيجة اقتراح لجنة الأوراق المالية والبورصة SEC الإفصاح الإلزامي عن سياسات إدارة المخاطر السيبرانية للشركات العامة في مارس ٢٠٢٢)، وذلك باستخدام تصميم تجريبي بين المشاركين ٤ × ١، لفحص ما إذا كانت إدراكات المستثمرين غير المحترفين وقراراتهم تختلف بين استراتيجيات إدارة

المخاطر السيبرانية وهي التقييم الذاتي، والتقييم الذاتي بالإشارة إلى إطار المعهد الوطني للمعايير والتكنولوجيا (NIST)، والتوكيد من طرف ثالث، والتأمين ضد مخاطر الأمن السيبراني.

تم الاستعانة بـ ١٥١ مشاركًا من خلال منصة Cloud Research Connect كمصدر للحصول على المشاركين لدراسات البحث. وتم تحديد المقيمون في الولايات المتحدة، بين سن ١٨ و٧٥ عامًا، مع حصولهم على تعليم من بعض الكليات إلى درجة مهنية، باعتبارهم كمستثمرين غير محترفين.

وأشارت نتائج الدراسة أن استعداد المستثمرين غير المحترفين للاستثمار أعلى بكثير بالنسبة لاستراتيجية التأمين (استخدام منشأة متخصصة) مقارنة بالتوكيد على أنشطة الأمن السيبراني من طرف ثالث، والتقييم الذاتي، والتقييم الذاتي بالإشارة إلى إطار المعهد الوطني للمعايير والتكنولوجيا (NIST). وتوضح نتائج الدراسة أن إدراكات المستثمرين عن المخاطر المالية نتيجة الأمن السيبراني تعدل من تأثير فعالية استراتيجية إدارة المخاطر السيبرانية على العلاقة بين استراتيجية إدارة المخاطر السيبرانية واحتمالية الاستثمار.

كما هدفت دراسة Romanosky and Sayers (2024) إلى اختبار كيفية دمج الشركات لمخاطر الأمن السيبراني في ممارسات إدارة المخاطر بالشركات مع تزايد وشدة اختراقات الأمن السيبراني، حيث أصبحت مخاطر الأمن السيبراني مصدر قلق للشركات لذلك ازدادت أهمية معالجة الشركات لمخاطر الأمن السيبراني بشكل فعال داخل استراتيجيات إدارة المخاطر الشاملة للشركات. أجرى الباحثان مقابلات شبه منظمة مع مديري إدارة المخاطر من شركات مختلفة لجمع أراءهم عن ممارسات إدارة المخاطر للشركات وطرق دمج مخاطر الأمن السيبراني.

وأشارت نتائج الدراسة إلى وجود تنوع في ممارسات إدارة المخاطر بالشركات. كما أوضحت نتائج الدراسة إلى أنه على الرغم من حداثة مخاطر الأمن السيبراني إلا أن العديد من الشركات دمجت هذه المخاطر ضمن أطر عمل إدارة المخاطر المؤسسية بالشركات. وصنفت معظم الشركات مخاطر الأمن السيبراني باعتبارها مخاطر تشغيلية مثل المخاطر الأخرى مثل حوادث مكان العمل أو التلاعب، وليس باعتبارها مخاطر استراتيجية ناشئة عن التطورات التكنولوجية. وأشارت نتائج الدراسة إلى عدم وجود معالجة متخصصة لإدارة مخاطر الأمن السيبراني، ومعالجة تلك المخاطر داخل أطر عمل إدارة مخاطر الشركات الحالية دون الحاجة إلى عمليات أو تعديلات متخصصة.

ويوفر هذا البحث رؤى قيمة للشركات التي تسعى إلى إدارة مخاطر الأمن السيبراني بدمجها بإدارة مخاطر للشركة ككل.

وبناء على الدراسات السابقة، يتضح اختلاف أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والإفصاح عن تلك الاختراقات، وقرار الاستثمار في الشركات التي تم اختراقها مع ندرة الدراسات التي ركزت على الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني، وبالتالي يمكن صياغة **الفرضين الثالث والرابع كما يلي:**

H_3: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الاختراقات السيبرانية والاستثمار في الشركات المصرية

H3a: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات المصرية

H3b: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الاختراقات السيبرانية وقيمة الاستثمار في الشركات المصرية

H4: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية والاستثمار في الشركات المصرية

H4a: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية و قرار الاستثمار في الشركات المصرية

H4b: يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقيمة الاستثمار في الشركات المصرية

٥/٦- منهجية البحث:

قام الباحث باختبار فروض الدراسة باستخدام المدخل التجريبي قياساً على بعض الدراسات(Huang and Murthy 2024; Cheng et al. 2022) وذلك بالقيام بدراسة حالات تجريبية، وتحليل نتائج المقارنات بين تلك الحالات، ولتحقيق هذا الهدف سيتم عرض مجتمع وعينة الدراسة وتوصيف وقياس متغيرات الدراسة، ونموذج الدراسة والمعالجات التجريبية والمقارنات بين المعالجات، والأساليب الاحصائية المستخدمة لاختبار فروض الدراسة، وذلك على النحو التالي:

٦/ ٥/١- مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من الأكاديميين وطلاب الدراسات العليا في مجال المحاسبة والمراجعة باعتبارهم ممثلين عن المستثمرين غير المحترفين بما يتفق مع دراسة (2023) Demk and Kapla، وذلك بافتراض إمكانية معرفتهم بالإفصاحات عن الاختراقات السيبرانية والإفصاح عن إدارة مخاطر الأمن السيبراني، والعوامل المؤثرة على قرار الاستثمار في الشركات التي تعرضت لتلك الاختراقات ومدى الاعتماد على افصاحات الشركات عن الاختراقات والإفصاح عن إدارة المخاطر السيبرانية.

٦/ ٥/ ٢- ادوات وإجراءات الدراسة:

تتضمن أدوات الدراسة الحالات التجريبية المبنية على التقارير المالية الفعلية لأحدى الشركات المقيدة بالبورصة المصرية وتقرير إدارة المخاطر السيبرانية والاسئلة المرافقة لهذه الحالات. واعتمد الباحث على التصميم التجريبي (٢x٢x٢) قياساً على دراستي (كعموش٢٠٢٤، القاضي ٢٠٢٤) بهدف اختبار العلاقة محل الدراسة، حيث تم صياغة إطار مقترح للأثر المعدل الإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين اختراقات الأمن السيبراني، والإفصاح عنها، وقرار الاستثمار في الشركات التي تعرضت للاختراقات السيبرانية.

٦/٥/٢/١- توصيف وقياس متغيرات الدراسة:

بالرجوع لفروض الدراسة يمكن تحديد وقياس المتغيرات المستقلة والتابعة كما يلي:

١- المتغيران المستقلان:

- **الاختراقات السيبرانية** ويتم قياسها من خلال صياغة حالات تجريبية تعبر عن وجود أو عدم وجود اختراقات سيبرانية بالشركة، بما يتفق مع دراسة (Demk and Kaplan 2023).

- **الإفصاح عن الاختراقات السيبرانية** ويتم قياسهما من خلال صياغة حالات تجريبية تقارن بين وجود افصاح أو عدم وجود افصاح عن الاختراقات السيبرانية، بما يتفق مع دراسة (Romanosky and Sayers2024).

ب- المتغير المعدل:

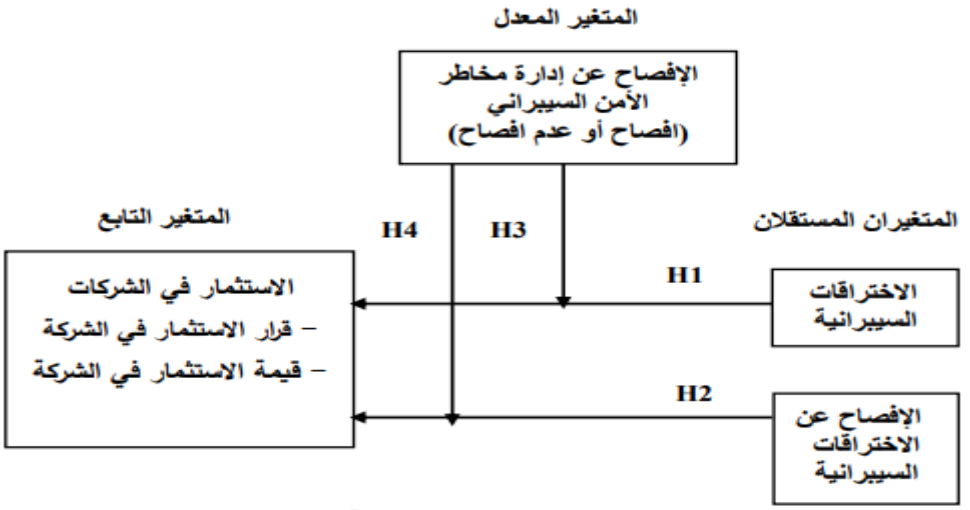
تم استخدام **الافصاح عن إدارة المخاطر السيبرانية** بتقديم تقرير إدارة الشركة عن إدارة مخاطر الأمن السيبراني، ويشمل التقرير **وصف الإدارة** لبرنامج إدارة مخاطر الأمن السيبراني بالاستعانة بمعايير وصف برنامج إدارة مخاطر الأمن السيبراني، **وتأكيدات الإدارة** بأن التقرير يتم وفق معايير الوصف ووفق معايير خدمات الثقة، **ووجود رأي مراقب حسابات** مستقل عن فحص ومراجعة تقرير

الشركة عن إدارة المخاطر السيبرانية، بما يتفق مع إطار (AICPA,2017;Huang and Murthy 2024).

ج- المتغير التابع:

الاستثمار في الشركات، وذلك بتحديد مدى الاعتماد على الإفصاحات عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني **لاتخاذ قرار الاستثمار، وقيمة الاستثمارات في الشركة،** بما يتسق مع دراسة(Cheng et al. 2022).

ويمكن توضيح أثر الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والإفصاح عنها وقرار الاستثمار في الشركات، بالشكل التالي:



شكل رقم ١ : نموذج الدراسة

إعداد الباحث

٣/٥/٦. وصف وإجراءات الحالات التجريبية والتصميم التجريبي:

سيتناول الباحث في هذا الجزء وصف واجراءات الحالات التجريبية والتصميم التجريبي وذلك كما يلي:

٦-٥-٣-١ وصف وإجراءات الحالات التجريبية:

لإجراء الدراسة التجريبية تم تصميم شركة تعمل ضمن قطاع الاتصالات والاعلام وتكنولوجيا المعلومات في البورصة المصرية، وعرضها على المشاركين بشكل عشوائي، وأعد الباحث تصميم تجريبي (٢x٢ x٢) يتضمن ٨ حالات تجريبية تستوعب المعالجات المختلفة للمتغيرين المستقلين مع المتغير المعدل للعلاقة محل الدراسة:

الحالة الأولي: تعرض الشركة لاختراق سيبراني لنظام حسابات العملاء، ولم يتم الافصاح عن إدارة مخاطر الأمن السيبراني.

الحالة الثانية: تعرض الشركة لاختراق سيبراني لنظام حسابات العملاء، مع الإفصاح عن إدارة مخاطر الأمن السيبراني وسياساته واجراءاته.

الحالة الثالثة: لم تتعرض الشركة لاختراق سيبراني لنظام حسابات العملاء، مع عدم وجود إفصاح عن إدارة مخاطر الأمن السيبراني.

الحالة الرابعة: لم تتعرض الشركة لاختراق سيبراني لنظام حسابات العملاء، مع الإفصاح عن إدارة مخاطر الأمن السيبراني وسياساته وإجراءاته.

الحالة الخامسة: تعرض الشركة لاختراق سيبراني، وتم الإفصاح عن الاختراق السيبراني، مع عدم وجود إفصاح عن إدارة مخاطر الأمن السيبراني.

الحالة السادسة: تعرض الشركة لاختراق سيبراني، وتم الإفصاح عن الاختراق السيبراني، مع وجود إفصاح عن إدارة مخاطر الأمن السيبراني وسياساته وإجراءاته.

الحالة السابعة: تعرض الشركة لاختراق سيبراني، مع عدم وجود افصاح عن الاختراقات السيبرانية، وعدم وجود إفصاح عن إدارة مخاطر الأمن السيبراني.

الحالة الثامنة: تعرض الشركة لاختراق سيبراني، وتم الإفصاح عن عدم وجود اختراقات سيبرانية، وتم الإفصاح عن إدارة مخاطر الأمن السيبراني وسياساته واجراءاته.

طلب من المشاركين في عينة الدراسة الإجابة على بعض الأسئلة التي تهدف إلى مدى الاعتماد على المعلومات المقدمة لقرار الاستثمار، وتأثير المعلومات على سعر سهم الشركة. إضافة إلى مجموعة من الأسئلة لأغراض التحليلات الإضافية تتعلق بتحليل العوامل المؤثرة على قراري الشركة بالإفصاح عن التعرض لاختراق سيبراني، والإفصاح عن إدارة مخاطر الأمن السيبراني، وذلك مع مجموعة من الأسئلة– تم إدراجها في بداية الحالة التجريبية–تهدف إلى قياس بعض الخصائص الديموغرافية لمفردات العينة، مثل؛ النوع، المركز الوظيفي، مستوى الخبرة.

٢/٣/٥/٦ التصميم التجريبي:

استخدم الباحث لقياس أثر الإفصاح عن إدارة مخاطر الأمن السيبراني كمتغير معدل للعلاقة بين الافصاح عن الاختراقات السيبرانية وقرار الاستثمار في تلك الشركات تصميماً تجريبياً (٢x٢x٢) بين المجموعات، وذلك على النحو المبين في الجدول التالي:

جدول رقم ١التصميم التجريبي

المتغير المعدل / المتغيران المستقلان		عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني	وجود افصاح عن إدارة مخاطر الأمن السيبراني
الاختراق السيبراني	حدث	حالة رقم (١) قرار وقيمة الاستثمار	حالة رقم (٢) قرار وقيمة الاستثمار
	لم يحدث	حالة رقم (٣) قرار وقيمة الاستثمار	حالة رقم (٤) قرار وقيمة الاستثمار
الافصاح عن الاختراقات السيبرانية	تم الإفصاح	حالة رقم (٥) قرار وقيمة الاستثمار	حالة رقم (٦) قرار وقيمة الاستثمار
	لم يتم الإفصاح	حالة رقم (٧) قرار وقيمة الاستثمار	حالة رقم (٨) قرار وقيمة الاستثمار

وفقاً لوصف الحالات التجريبية والتصميم التجريبي تظهر الـ ٨ معالجات التجريبية على النحو التالي:

المعالجة رقم (١):	وجود اختراقات سيبرانية/ عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٢):	وجود اختراقات سيبرانية/ وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٣):	عدم وجود اختراقات سيبرانية/ عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٤):	عدم وجود اختراقات سيبرانية/ عدم جود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٥):	وجود افصاح عن الاختراقات السيبرانية/ عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٦):	وجود افصاح عن الاختراقات السيبرانية/ وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٧):	عدم وجود افصاح عن الاختراقات السيبرانية/ عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.
المعالجة رقم (٨):	عدم وجود افصاح عن الاختراقات السيبرانية/ وجود افصاح عن إدارة مخاطر الأمن السيبراني/ قرار وقيمة الاستثمار في الشركة.

المقارنات بين المعالجات:

ولاختبار فروض الدراسة، تم إجراء المقارنات التالية بين نتائج المعالجات لاختبار الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والإفصاح عنها وقرار وقيمة الاستثمار في الشركات، وذلك كما يلي:

المقارنة الأولي: لاختبار فرض الدراسة الأول (H1) سيتم مقارنة الحالات (2+1) مع الحالات (3+4).

المقارنة الثانية: لاختبار فرض الدراسة الثاني (H2) سيتم مقارنة الحالات (6+5) مع الحالات (7+8).

المقارنة الثالثة: لاختبار فرض الدراسة الثالث (H3) سيتم مقارنة الحالات (1x3) مع الحالات (2x4).

المقارنة الرابعة: لاختبار فرض الدراسة الرابع (H4) وسيتم مقارنة الحالات (5x7) مع الحالات (6x8).

٦/٦- نتائج الدراسة التجريبية:

يتضمن هذا القسم وصف بيانات المشاركين في عينة الدراسة، وعرض وتحليل الإحصاءات الوصفية لمتغيرات الدراسة والاختبارات الإحصائية للتأكد من اعتدالية بيانات الدراسة بهدف تحديد نوع الاختبارات الإحصائية الملائمة لاختبار الفروض. كما يهدف هذا القسم إلى عرض وتحليل نتائج الاختبارات الإحصائية لاختبار فروض الدراسة، ونتائج التحليل الإضافي.

١/٦/٦- وصف عينة الدراسة ونتائج الإحصاء الوصفي لعينة الدراسة:

١/١/٦/٦- وصف عينة الدراسة ونتائج الإحصاء الوصفي لعينة الدراسة:

يتضمن الجدول التالي عرض ملخص بيانات المشاركين في عينة الدراسة:

جدول رقم (٢)

بيان	عدد الحالات التجريبية الموزعة	عدد الحالات التجريبية المستلمة	نسبة الردود على الحالات المستلمة	عدد الردود المكتملة	نسبة الردود المكتملة إلى الردود المستلمة
عينة الأكاديميين	70	55	78%	52	74%

ويوضح الجدول رقم (٣) الإحصاء الوصفي لعينة الدراسة على النحو التالي:

جدول رقم (٣)

البيان	النسبة	البيان	النسبة	البيان	النسبة
النوع		الوظيفة		مستوى الخبرة	
ذكر	75%	طالب دراسات عليا	15%	أقل من سنة	%5
انثي	25%	عضو هيئة تدريس	85%	من سنة إلى أقل من ٣ سنوات	%5
				من ٣ سنوات إلى أقل من ٥ سنوات	%5
				من ٥ سنوات الي ١٠ سنوات	%10
				١٠ سنوات فأكثر	%75

ويتضح من الجدول السابق أن الجزء الأكبر من عينة الدراسة من أعضاء هيئة التدريس حيث تمثل 85% من عينة الدراسة، كما أن خبرة 75% من عينة الدراسة تتجاوز 10 سنوات.

٢/١/٦/٦- اختبار الاعتدالية:

لتحديد نوع توزيع المجتمع الذي تم سحب عينة الدراسة منه، ونوع الاختبارات معلميه Parametric أو لا معلميه Non-parametric، تم اجراء اختبار Kolmogrov-Smirnov واختبار Shapiro-Walk لمعرفة إذا كان هذا التوزيع يتبع التوزيع الطبيعي أم لا. وتم صياغة الفرض الاحصائي لهذا الاختبار على النحو التالي:

- فرض العدم H_0: بيانات العينة مسحوبة من مجتمع له توزيع طبيعي.
- الفرص البديل H_1: بيانات العينة مسحوبة من مجتمع ليس له توزيع طبيعي.

الجدول رقم (٤) اختبار الاعتدالية

	Kolmogrov-Smirnov		Shapiro-Walk	
	Statistics	P-value	Statistics	P-value
الحالة الأولي	0.256	0.00	0.82	0.00
الحالة الثانية	0.287	0.00	0.377	0.00
الحالة الثالثة	0.271	0.00	0.2717	0.00
الحالة الرابعة	0.189	0.00	0.909	0.00
الحالة الخامسة	0.269	0.00	0.270	0.00
الحالة السادسة	0.188	0.00	0.890	0.00

وقد أظهرت النتائج الخاصة بالتحليل كما هو موضح بالجدول رقم (٤) أن مستوى المعنوية لجميع حالات الدراسة أقل من 0.05 مما يعني رفض فرض العدم وقبول الفرض البديل أي ان

البيانات لا تتبع التوزيع الطبيعي، وبالتالي تم استخدام أحد الأساليب اللامعلمية Non-Parametric لاختبار فروض الدراسة.

٢/٦/٦- نتائج اختبار فروض الدراسة:

يهدف هذا القسم إلى عرض نتائج اختبار فروض الدراسة باستخدام الاختبارات اللامعلمية، لتحليل العلاقة بين الافصاح عن الاختراقات السيبرانية وقرار الاستثمار في الشركات، وأثر الإفصاح عن إدارة المخاطر السيبرانية على العلاقة بين الافصاح عن الاختراقات السيبرانية وقرار الاستثمار في الشركات.

أولا: التحليل الأساسي:

لاختبار فروض البحث، قام الباحث باستخدام اختبار Wilcoxon Sum Rank test اللامعلمي[١] للتحقق من العلاقة محل الدراسة وذلك على النحو التالي:

١/٢/٦/٦- نتيجة اختبار الفرض الأول:

استهدف الفرض الأول (H1) اختبار أثر الاختراقات السيبرانية على الاستثمار في تلك الشركات، وذلك من خلال مقارنة الحالتين (2+1) حدوث الاختراقات السيبرانية (مع الإفصاح أو عدم الافصاح عن إدارة مخاطر الأمن السيبراني) مع الحالات (4+3) عدم حدوث اختراقات سيبرانية (مع الإفصاح أو عدم الافصاح عن إدارة مخاطر الأمن السيبراني). ويوضح الجدول رقم (٥) نتيجة اختبار Wilcoxon Sum rank وذلك على النحو التالي:

الجدول رقم (٥) نتيجة اختبار Wilcoxon Signed rank test لأثر الاختراقات السيبرانية على الاستثمار في الشركات المصرية

المقارنات	قيمة Z	P-Value	الرتب الموجبة والسالبة	قيم الرتب	متوسط الرتب	مجموع الرتب
بالنسبة لقرار الاستثمار في الشركات	-5.983	.000	Negative Ranks Positive Ranks Ties Total	4 41 7 52	4 24.85	16 1019
بالنسبة لقيمة الاستثمار في الشركات	-4.910	.000	Negative Ranks Positive Ranks Ties Total	6 41 5 52	19 24.73	114 1014

١) قياساً على (Boolaky and Quick (2016);Balafoutas et al.(2020)

وقد أظهرت نتائج الجدول رقم (٥) وجود اختلافات معنوية بين حالات الدراسة التجريبية بالنسبة لأثر الاختراقات السيبرانية على **قرار الاستثمار** بالشركة (Z= - 5.983, P-value=0.000)، **ولتحديد اختلاف اتجاه قرار الاستثمار** بين المجموعتين التجريبيتين، تم استخدام Ranks في اختبار Wilcoxon Signed rank test، حيث مجموع الرتب السالبة ١٦ بالمقارنة بمجموع الرتب الموجبة ١٠١٩ بما يشير إلى رفض المشاركين في التجربة للاستثمار في الشركات التي تعرضت لاختراق سيبراني بدرجة أكبر مقارنة بالشركات التي لم تتعرض للاختراقات السيبرانية، ومن ثم **قبول الفرض H1a**، وكذلك بالنسبة لأثر الاختراقات السيبرانية على **قيمة الاستثمار** (Z= - 4.91, P-value=0.00) ، **وبشأن اتجاه الاختلافات** بين اثر الاختراقات السيبرانية على قيمة الاستثمار بين المجموعتين التجريبيتين تم استخدام Ranks في اختبار Wilcoxon Signed rank test،حيث مجموع الرتب السالبة ١١٤بالمقارنة بمجموع الرتب الموجبة ١٠١٤ بما يشير إلى انخفاض قيمة الاستثمار في الشركات التي تعرضت لاختراق سيبراني مقارنة بالشركات التي لم تتعرض للاختراقات السيبرانية، ومن ثم **قبول الفرض H1b.** وبناء على ما سبق، **تم قبول الفرض الأولH1 بأنه تؤثر اختراقات الأمن السيبراني بصورة سلبية معنوية على الاستثمار بالشركات المصرية** بما يتفق مع دراسة (Jiang et al. 2022).

ويرى الباحث أنه يمكن تفسير النتائج باعتبار أن الاختراقات السيبرانية تعد مؤشراً سلبياً على جودة هيكل الرقابة الداخلية بالشركة وأنظمتها الالكترونية وسمعة الشركة، بما يؤدي إلى عدم تفضيل المستثمرين للاستثمار في الشركات التي تعرضت لاختراقات سيبرانية، وتخفيض الاستثمارات السابقة في تلك الشركات.

٢/٢/٦/٦- نتيجة اختبار الفرض الثاني:

استهدف الفرض الثاني(H2) اختبار مدى وجود أثر سلبي للإفصاح عن الاختراقات السيبرانية على الاستثمار في الشركات، وذلك من خلال مقارنة الحالتين (6+5) الإفصاح مقابل عدم الافصاح عن إدارة مخاطر الأمن السيبراني، والإفصاح عن الاختراقات السيبرانية) مع الحالتين (8+7) الإفصاح مقابل عدم الافصاح عن إدارة مخاطر الأمن السيبراني، وعدم الإفصاح عن الاختراقات السيبرانية. ويوضح الجدول رقم (٦) نتيجة اختبار Wilcoxon Sum rank، وذلك على النحو التالي:

الجدول رقم (٦) نتيجة اختبار Wilcoxon Signed rank test لأثر الافصاح عن الاختراقات السيبرانية على الاستثمار في الشركات المصرية

المقارنات	قيمة Z	P-Value	الرتب الموجبة والسالبة	قيم الرتب	متوسط الرتب	مجموع الرتب
بالنسبة لقرار الاستثمار في الشركات	-3.636	0.001	Negative Ranks	36	22.28	802.00
			Positive Ranks	8	23.50	188.00
			Ties	8		
			Total	52		
بالنسبة لقيمة الاستثمار في الشركات	-2.059	0.039	Negative Ranks	32	20.94	670.00
			Positive Ranks	12	26.67	320.00
			Ties	8		
			Total	52		

وقد أظهرت نتائج الجدول رقم (٦) وجود اختلافات معنوية بين حالات الدراسة التجريبية بالنسبة لدور الإفصاح عن الاختراقات السيبراني على **قرار الاستثمار** بالشركة (Z= - 3.636, P-value=0.001) ، **ولتحديد اختلاف اتجاه قرار الاستثمار** بين المجموعتين التجريبيتين تم استخدام Ranks في اختبار Wilcoxon Signed rank test، حيث مجموع الرتب السالبة 802 بالمقارنة بمجموع الرتب الموجبة 188 بما يشير إلى رفض المشاركين في التجربة للاستثمار في الشركات التي تعرضت لاختراق سيبراني ولم تقم بالإفصاح عن تلك الاختراقات بدرجة أكبر مقارنة بالشركات التي قامت بالإفصاح عن الاختراقات السيبرانية ومن ثم **قبول الفرض H2a**، وكذلك بالنسبة لأثر الإفصاح عن الاختراقات السيبرانية على **قيمة الاستثمار** (Z= - 2.059, P-value=0.039)، **ولتحديد اتجاه الاختلافات** بين أثر الاختراقات السيبرانية على **قيمة الاستثمار** بين المجموعتين التجريبيتين، تم استخدام Ranks في اختبار Wilcoxon Signed rank test ،حيث مجموع الرتب السالبة 670 بالمقارنة بمجموع الرتب الموجبة 320 بما يشير إلى انخفاض قيمة الاستثمار في الشركات التي تعرضت لاختراق سيبراني ولم تقم بالإفصاح عن تلك الاختراقات مقارنة بالشركات التي قامت بالإفصاح عن الاختراقات السيبرانية، وتعرضت لاختراقات سيبرانية، ومن ثم **قبول الفرض H2b** . وبناء على ما سبق، **تم قبول الفرض الثانيH2 بأنه يؤثر الافصاح عن اختراقات الأمن السيبراني بصورة سلبية معنوية على الاستثمار بالشركات المصرية** بما يتفق مع دراسة (Jiang et al. 2022).

ويمكن ملاحظة أن الإفصاح عن الاختراقات السيبرانية يؤثر **بصورة سلبية** على قرار وقيمة الاستثمار بالشركة باعتباره افصاح لاحق لحدوث تلك الاختراقات، وبالتالي يمكن القول بإنه قد لا يضيف قيمة لأصحاب المصالح بالشركة، خاصة في حالة توصل أصحاب المصالح بالشركة لأنباء عن الاختراقات السيبرانية بصورة مسبقة من مصادر بخلاف افصاحات الإدارة عن الاختراقات السيبرانية، بما يخفض من القيمة المعلوماتية لتلك الإفصاحات بالنسبة لأصحاب المصالح بالشركة مع تأخر تلك الإفصاحات.

٣/٢/٦/٦- نتيجة اختبار الفرض الثالث:

استهدف الفرض الثالث تحليل أثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الاختراقات السيبراني وقرار الاستثمار في الشركات المصرية، وذلك من خلال مقارنة الحالتين (1x3) حالتي حدوث اختراق مقابل عدم حدوث اختراق/عدم وجود إفصاح عن إدارة مخاطر الأمن السيبراني مع الحالتين (2x4) حالتي حدوث اختراق مقابل عدم حدوث اختراق/ الإفصاح عن إدارة مخاطر الأمن السيبراني. ويوضح الجدول التالي نتيجة اختبار Wilcoxon Sum rank، وذلك على النحو التالي:

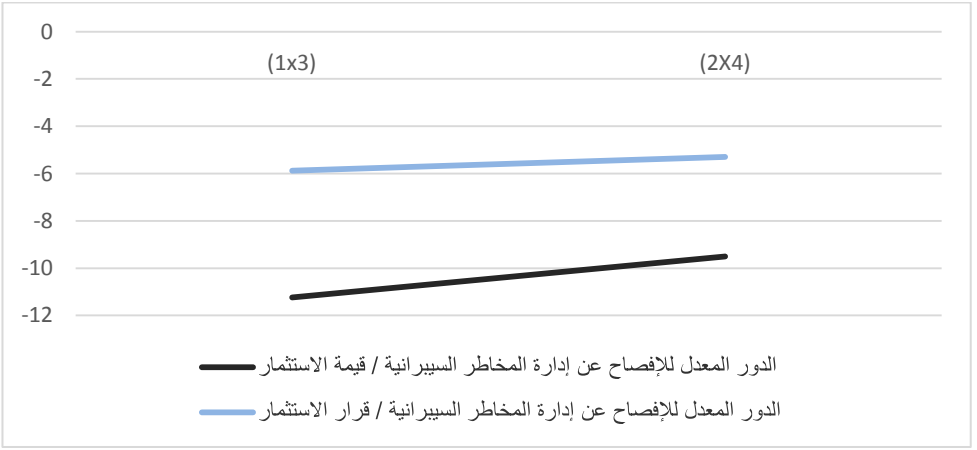
جدول رقم (٧) نتيجة اختبار Wilcoxon Signed rank testلأثر الافصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات

المقارنات	الأثر التفاعلي	قيمة Z	P-Value	الرتب الموجبة والسالبة	قيم الرتب	متوسط الرتب	مجموع الرتب
بالنسبة لقرار الاستثمار في الشركات	الحالات (1x3) مع الحالات (2x4)	-5.8	0.00	Negative Ranks Positive Ranks Ties Total	8 40 4 52	4.5 28.5	36 1140
		-5.3	0.00	Negative Ranks Positive Ranks Ties Total	9 38 5 52	11.33 27.0	102 1026
بالنسبة لقيمة الاستثمار في الشركات	الحالات (1x3) مع الحالات (2x4)	-5.35	0.00	Negative Ranks Positive Ranks Ties Total	3 39 10 52	12.5 22.2	37.5 865.5
		-4.629	0.00	Negative Ranks Positive Ranks Ties Total	4 40 8 52	26.5 22.1	106 884

ولاختبار الفرض الثالث (H3) بأن " **يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الاختراقات السيبرانية والاستثمار في الشركات المصرية**". قام الباحث بمقارنة معنوية الفروق بين متوسط الحالات الأولي والثالثة (1x3) ومتوسط الحالات الثانية والرابعة (2x4). وقد أظهرت نتائج الجدول رقم (٧) بوجود أثر معنوي للاختراقات السيبرانية على قرار الاستثمار في الشركات حيث أن (Z=-5.8,P-value=0.00;Z=-5.3, P-value=0.00) لكل منهم على التوالي. وتشير هذه النتائج إلى عدم وجود تأثير للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات (عدم وجود اختلاف في التأثير السلبي للاختراقات السيبرانية سواء في حالة الإفصاح أو عدم الإفصاح عن إدارة مخاطر الأمن السيبراني)، ومن **ثم عدم قبول الفرض H3a**، بما يتوافق مع دراسة Cheng et al. (2022).

كما أظهرت نتائج الجدول رقم (٧) وجود أثر معنوي للاختراقات السيبرانية على قيمة الاستثمار في الشركات حيث أن (Z=-5.35,P-value=0.00;Z=-4.629,P-value=0.00) لكل منهم على التوالي. وتشير هذه النتائج إلى عدم وجود تأثير للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقيمة الاستثمار في الشركات (عدم وجود اختلاف في التأثير السلبي للاختراقات السيبرانية سواء في حالة الإفصاح أو عدم الإفصاح عن إدارة مخاطر الأمن السيبراني)، **ومن ثم عدم قبول الفرض H3b**. وبناء على النتائج السابقة، **تم رفض الفرض الثالث H3 بالنسبة** للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية والاستثمار في الشركات، بما يتفق مع دراسة (Sari et al. 2024).

ويمكن **ملاحظة** عدم معنوية الدور المعدل **للإفصاح عن إدارة مخاطر الأمن السيبراني** على العلاقة بين الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات، نتيجة حداثة وعدم انتشار **هذا الإفصاح**، ووجود مستثمرين غير محترفين ضمن عينة الدراسة. ويمكن تلخيص أثر الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات، وذلك من جانب الاعتماد على المعلومات التي تم الافصاح عنها وقيمة الاستثمار في تلك الشركات بالشكل التالي:



شكل رقم٢ : أثر الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات

وتوضح نتائج الشكل رقم (٢) عدم وجود أثر معدل معنوي للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات التي تم اختراقها، بما يتفق مع دراسة (Demk and Kaplan,2023)، بما يبين حداثة الإفصاحات عن إدارة مخاطر الأمن السيبراني وانخفاض تأثيرها المعدل على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات.

٤/٢/٦/٦ – نتيجة اختبار الفرض الرابع:

استهدف الفرض الرابع تحليل أثر **الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار الاستثمار في الشركات المصرية**، وذلك من خلال مقارنة الحالتين (5x7) حالتي الإفصاح عن الاختراقات السيبرانية مقابل عدم الإفصاح عن الاختراقات السيبرانية/عدم وجود افصاح عن إدارة مخاطر الأمن السيبراني مع الحالتين (6x8) حالتي الإفصاح عن الاختراقات السيبرانية مقابل عدم الإفصاح عن الاختراقات السيبرانية/ وجود افصاح عن إدارة مخاطر الأمن السيبراني، ويوضح الجدول التالي نتيجة اختبار Wilcoxon Sum rank وذلك على النحو التالي:

جدول رقم (٨) نتيجة اختبار Wilcoxon Signed rank test لأثر الافصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار الاستثمار في الشركات المصرية

المقارنات	الأثر التفاعلي	قيمة Z	P-Value	الرتب الموجبة والسالبة	قيم الرتب	متوسط الرتب	مجموع الرتب
بالنسبة لقرار الاستثمار في الشركات	الحالات (5x7) مع الحالات (6x8)	-1.951	.055	Negative Ranks	23	15.04	346.00
				Positive Ranks	8	18.75	150.00
				Ties	21		
				Total	52		
		-3.779	0.00	Negative Ranks	28	16.57	464.00
				Positive Ranks	4	16.00	64.00
				Ties	20		
				Total	52		
بالنسبة لقيمة الاستثمار في الشركات	الحالات (5x7) مع الحالات (6x8)	-.046	.963	Negative Ranks	25	17.08	427.00
				Positive Ranks	16	27.13	434.00
				Ties	11		
				Total	52		
		-3.240	.001	Negative Ranks	28	15.43	432.00
				Positive Ranks	4	24.00	96.00
				Ties	20		
				Total	52		

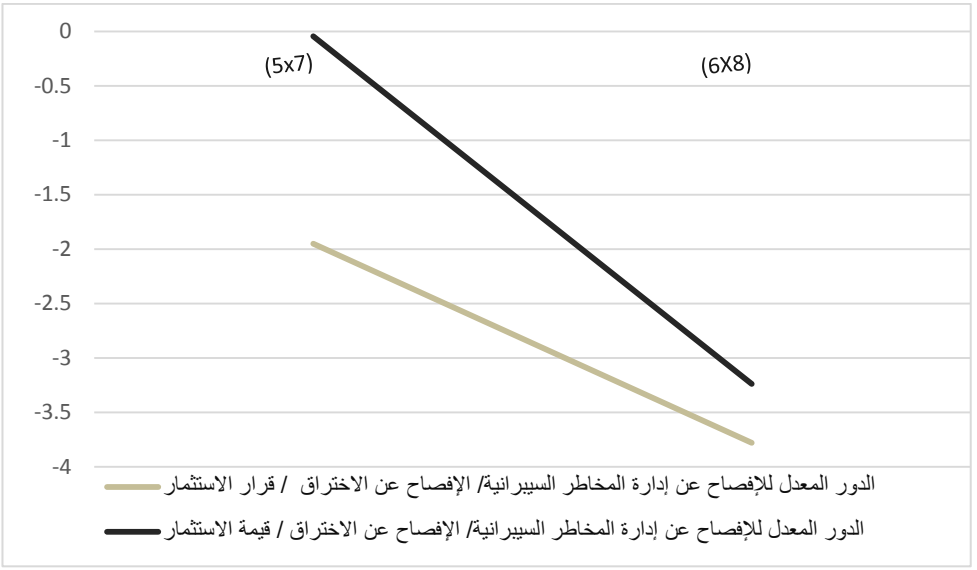
ولاختبار الفرض الرابع (H4) بأنه " يؤثر **الإفصاح عن إدارة مخاطر الأمن السيبراني بالشركات على العلاقة بين الإفصاح عن الاختراقات السيبرانية والاستثمار في الشركات المصرية**". قام الباحث بمقارنة معنوية الفروق بين متوسط الحالات الخامسة والسابعة(5x7) ومتوسط الحالات السادسة والثامنة (6x8) **بالنسبة لقرار الاستثمار في الشركات.** وقد أظهرت نتائج الجدول رقم (8) إلى وجود اختلافات ذات دلاله معنوية بين متوسط إجابات الحالتين الخامسة والسابعة مقابل متوسط إجابات الحالتين السادسة والثامنة حيث أن (Z=−1.951,P−value=0.055; Z=−3.779.3,P−value=0.00)

بما يشير إلى وجود أثر معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية **وقرار الاستثمار** في الشركات **ومن ثم قبول الفرض H4a.**

كما قام الباحث بمقارنة معنوية الفروق بين متوسط الحالات الخامسة والسابعة (5x7) ومتوسط الحالات السادسة والثامنة (6x8) **بالنسبة لقيمة الاستثمار في الشركات.** وقد أظهرت نتائج الجدول رقم (8) إلى وجود اختلافات ذو دلاله معنوية بين متوسط إجابات الحالتين الخامسة والسابعة مقابل متوسط إجابات الحالتين السادسة والثامنة حيث أن (Z=−0.046,P−value=0.963; Z= −3.240,P−value=0.00) بما يشير إلى وجود أثر معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقيمة الاستثمار في الشركات، **ومن ثم قبول الفرض H4b.** وبناء على النتائج السابقة، **تم قبول الفرض الرابع H4 بوجود أثر معنوي** للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات، حيث أدى الإفصاح عن إدارة مخاطر الأمن السيبراني إلى تخفيض الأثر السلبي للإفصاح عن الاختراقات السيبرانية على قرار وقيمة الاستثمار في الشركات، وتتفق هذه النتائج مع دراسة Mazzoccoli (2023).

ويمكن القول إن الدور المعدل للإفصاح عن إدارة المخاطر السيبرانية لم يكن له أثر معنوي على العلاقة بين الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات، بينما اتضح وجود أثر معنوي للإفصاح عن إدارة المخاطر السيبرانية **مع** وجود افصاحات عن الاختراقات السيبرانية، بما قدم معلومات أكثر ملائمة للمستثمرين في الشركات خاصة بوجود سياسات وإجراءات واضحة لمعالجة الاختراقات السيبرانية التي تم الإفصاح عنها.

ويمكن تلخيص أثر الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين **الإفصاح عن الاختراقات السيبرانية وقرار وقيمة الاستثمار** في الشركات، بالشكل التالي:



شكل رقم٣: أثر الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاحات عن الاختراقات السيبرانية وقرار الاستثمار في الشركات

وتوضح نتائج الشكل رقم (٣) وجود أثر معدل معنوي للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات، بما يتفق مع دراسة (Huang and Murthy 2024)، حيث أدى الأثر المعدل الى تخفيض جزئي للأثار السلبية للإفصاح عن الاختراقات السيبرانية على قرار وقيمة الاستثمار في الشركات.

٣/٦/٦-الاختبارات الاضافية:

قام الباحث بتحليل واختبار العوامل المؤثرة على الافصاح عن الاختراقات السيبرانية، والإفصاح عن إدارة مخاطر الأمن السيبراني، وعلاقتها بقرار الاستثمار في الشركات، بالإضافة لاختبار أثر اختلاف الإفصاح وعدم الإفصاح عن إدارة مخاطر الأمن السيبراني على قرار الاستثمار بالشركات، في حالة الإفصاح عن الاختراقات السيبرانية، وذلك على النحو التالي:

١/٣/٦/٦– التحليل الاحصائي للعوامل المؤثرة على قرار الافصاح عن الاختراقات السيبرانية:

تم تحليل العوامل المؤثرة على الافصاح عن الاختراقات السيبرانية. وتم استخدام اختبار Wilcoxon –sum rank test لتحليل أهم تلك العوامل، كما يتضح بالجدول التالي:

جدول رقم (٩) تحليل العوامل المؤثرة على قرار الافصاح عن الاختراقات السيبرانية وعلاقتها بقرار الاستثمار في الشركة

البيان	قيمة الوسيط	P= value
- مستوى الثقة في مجلس الإدارة	4.0	0.01
-مستوى الثقة في الإفصاح عن الاختراقات السيبرانية	4.5	0.00
-قيمة الضرر الناتج على أصحاب المصالح بالشركة	4.5	0.00
-قوة نظام الرقابة الداخلية في الشركة التي تم اختراقها	4.5	0.00
-مدى أهمية الشركة في القطاع الذي تعمل به	4.0	0.01
-وجود قواعد أو قوانين ملزمة بالإفصاح عن الاختراقات السيبرانية	4.5	0.00
مقياس الموثوقية Cronbach's Alpha= 0.713		

وتشير نتائج اختبار Wilcoxon Sum rank test بالجدول رقم (٩) إلى أهمية كل من مستوى الثقة في مجلس الإدارة، ومدى أهمية الشركة في القطاع الذي تعمل به على الافصاح عن الاختراقات السيبرانية، **وبدرجة أكبر** كل من عوامل مستوى الثقة في الإفصاح عن الاختراقات السيبرانية، وقيمة الضرر الناتج على أصحاب المصالح بالشركة، وقوة نظام الرقابة الداخلية في الشركة التي تم اختراقها (قيمة الوسيط تتراوح بين 4.5 و4 وقيمة P-value تتراوح بين 0 و0.001). كما أوضحت نتائج التحليل الاحصائي زيادة الموثوقية لتلك النتائج، حيث مقياس الموثوقية Cronbach's Alpha= 0.713.

وبشأن الأكثر أهمية لمصدر الاختراقات السيبرانية عند الافصاح عن تلك الاختراقات اوضحت ٦٧% من عينة الدراسة (٣٥ مشارك من ٥٢) أهمية أثر القصور في الانظمة الداخلية للشركة باعتبارها مسبب لحدوث الاختراقات الداخلية أو الخارجية. وأشار بعض المشاركين في الدراسة أن **وجود قصور في هيكل الرقابة الداخلية وعدم وجود مراجع خارجي مستقل للتوكيد** على انظمة الشركة يزيد من احتمالية وقوع الاختراقات السيبرانية بالشركة. كما اوضح ٩٠ % (٤٧ مشارك من ٥٢) من المشاركين في الدراسة أن أكثر القطاعات أهمية للإفصاح عن الاختراقات السيبرانية هو القطاع المالي والبنكي ثم قطاع الاتصالات، ويفسر ذلك بكبر حجم هذه القطاع وزيادة أصحاب المصالح بهذا القطاع الذين يتأثرون بأضرار الاختراقات السيبرانية.

٢/٣/٦/٦- التحليل الاحصائي للعوامل المؤثرة على قرار الافصاح عن إدارة مخاطر الأمن السيبرانية وعلاقتها بقرار الاستثمار في الشركة

تم تحليل العوامل المؤثرة على الافصاح عن إدارة مخاطر الأمن السيبرانية. وتم استخدام اختبار Wilcoxon –sum rank test لتحليل أهم تلك العوامل، كما يتضح بالجدول التالي:

جدول رقم (١٠) تحليل العوامل المؤثرة على قرار الافصاح عن إدارة مخاطر الأمن السيبراني وعلاقتها بقرار الاستثمار في الشركة

البيان	قيمة الوسيط	P- value
- مدى خبرة اعضاء إدارة مخاطر الأمن السيبراني	3.5	0.02
- عمر إدارة مخاطر الأمن السيبراني	3.0	0.03
- مدى وجود سياسات واضحة لإدارة مخاطر الأمن السيبراني	4.5	0.00
- مدى وجود قوانين أو لوائح منظمة للإفصاح عن إدارة مخاطر الأمن السيبراني	5	0.00
- قيمة الاستثمارات في إدارة مخاطر الأمن السيبراني بالشركة	4.5	0.00
- توافر شهادات لمعايير أمن البيانات بالشركة مثل ISO22301 و ISO27001	4.0	0.01
- قوة النظم الرقابية بالشركة	4.5	0.00
- مدى وجود توكيد خارجي من مراقب حسابات على الافصاح عن إدارة المخاطر السيبرانية	4.5	0.00
مقياس الموثوقية Cronbach's Alpha = 0.703		

وتشير نتائج اختبار Wilcoxon Sum rank test بالجدول رقم (١٠) إلى أهمية كل من توافر شهادات لمعايير أمن البيانات بالشركة مثل ISO22301 و ISO27001، ومدى خبرة اعضاء إدارة مخاطر الأمن السيبراني، وعمر إدارة مخاطر الأمن السيبراني (قيمة الوسيط تتراوح بين 4 و3، قيمة P–value تتراوح بين 01. و 03 .0)، وبدرجة أكبر معنوية لكل من وجود قوانين أو لوائح منظمة للإفصاح عن إدارة مخاطر الأمن السيبراني، ووجود سياسات واضحة لإدارة مخاطر الأمن السيبراني، وقيمة الاستثمارات في إدارة مخاطر الأمن السيبراني بالشركة، وقوة النظم الرقابية بالشركة، ومدى وجود توكيد خارجي من مراقب حسابات مستقل على الافصاح عن إدارة المخاطر السيبرانية) قيمة الوسيط تتراوح بين 4.5 و 5 وقيمة P–value تساوي 0.00). كما أوضحت

نتائج التحليل الاحصائي زيادة الموثوقية لتلك النتائج، حيث مقياس الموثوقية Cronbach's Alpha= 0.713.

كما أشار ٩٠ % من المشاركين في الدراسة أن أكثر القطاعات أهمية للإفصاح عن إدارة مخاطر الأمن السيبراني هو القطاع المالي والبنكي ثم قطاع الاتصالات، ويفسر ذلك بكبر حجم هذه القطاع وزيادة اصحاب المصالح بهذا القطاع. كما أوضح أغلب المشاركين أهمية تكرار الإفصاح ووضوحه عن إدارة مخاطر الأمن السيبراني، وأهمية قرارات مجلس الإدارة والقوانين الملزمة لدعم الإفصاح عن إدارة مخاطر الأمن السيبراني.

٧/٦- النتائج والتوصيات والأبحاث المستقبلية:

يعرض الباحث فيما يلي لأهم النتائج والتوصيات ومجالات البحث المقترحة:

١/٧/٦- النتائج:

هدف البحث إلى تحليل واختبار العلاقة بين اختراقات الأمن السيبراني وقرار الاستثمار في الشركات المصرية، وتحليل الدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني، وعلى العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات المقيدة في البورصة المصرية.

وخلصت نتائج الدراسة التجريبية إلى وجود أثر سلبي معنوي لكل من الاختراقات السيبرانية والإفصاح عنها على قرار وقيمة الاستثمار بالشركات المصرية، ووجود أثر سلبي غير معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الاختراقات السيبرانية وقرار الاستثمار في الشركات، بينما اتضح وجود أثر معنوي للدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني على العلاقة بين الإفصاح عن الاختراقات السيبرانية وقرار وقيمة الاستثمار في الشركات، حيث يؤدي الإفصاح عن إدارة مخاطر الأمن السيبراني إلى تخفيض الأثر السلبي للإفصاح عن الاختراقات السيبرانية على قرار وقيمة الاستثمار في الشركات.

كما بينت نتائج التحليل الخاصة أهمية كل من مستوى الثقة في مجلس الإدارة، ومدى أهمية الشركة في القطاع الذي تعمل به على **الافصاح عن الاختراقات السيبرانية، وبدرجة أكبر** كل من عوامل مستوى الثقة في الإفصاح عن الاختراقات السيبرانية، وقيمة الضرر الناتج على أصحاب المصالح بالشركة، وقوة نظام الرقابة الداخلية في الشركة التي تم اختراقها. **وبشأن الأكثر أهمية لمصدر الاختراقات السيبرانية** عند الافصاح عن تلك الاختراقات، اتضح أهمية أثر الاخطاء في

الانظمة الداخلية للشركة باعتبارها مؤثر في حدوث الاختراقات الداخلية أو الخارجية. كما أشارت النتائج أن **وجود قصور في هيكل الرقابة الداخلية وعدم وجود مراجع خارجي مستقل للتوكيد** على انظمة الشركة يزيد من احتمالية وقوع الاختراقات السيبرانية بالشركة.

كما اتضح أهمية وجود قوانين أو لوائح منظمة للإفصاح عن إدارة مخاطر الأمن السيبراني، ووجود سياسات واضحة لإدارة مخاطر الأمن السيبراني، وقيمة الاستثمارات في إدارة مخاطر الأمن السيبراني بالشركة، وقوة النظم الرقابية بالشركة، ومدى وجود توكيد خارجي من مراقب حسابات مستقل على **الافصاح عن إدارة المخاطر السيبرانية**. كما أشارت نتائج الدراسة أن أكثر القطاعات أهمية للإفصاح عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني هو القطاع المالي والبنكي ثم قطاع الاتصالات، ويفسر ذلك بكبر حجم هذه القطاع وزيادة أصحاب المصالح بهذا القطاع المتأثرين بالاختراقات السيبرانية. كما خلصت نتائج التحليل الإضافي إلى وجود أثر معنوي سلبي للإفصاح عن الاختراقات السيبرانية على قرار الاستثمار في الشركات في حالة عدم الإفصاح عن إدارة مخاطر الأمن السيبراني على قرار الاستثمار بالشركات.

٦/٧/٢- التوصيات:

في ضوء ما انتهي اليه البحث من نتائج، يوصي الباحث بما يلي:

- ضرورة قيام هيئة الرقابة المالية بصياغة لوائح تنظيمية للإفصاح عن الاختراقات السيبرانية (بصورة وقتية مناسبة)، والإفصاح عن سياسات واستراتيجيات إدارة المخاطر السيبرانية
- إلزام هيئة الرقابة المالية للشركات بالإفصاح الإلزامي عن الاختراقات السيبرانية، والإفصاح عن سياسات واستراتيجيات وأنشطة إدارة المخاطر السيبرانية.
- ضرورة متابعة هيئة الرقابة المالية لإفصاحات الشركات عن الاختراقات السيبرانية في الوقت المناسب، والإفصاح عن إدارة مخاطر الأمن السيبراني.
- ضرورة تعديل المعايير المحاسبية ذات الصلة بإصدار معايير خاصة بالإفصاحات عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني.
- قيام جمعية المحاسبين والمراجعين المصرية بالتعاون مع أقسام المحاسبة بالجامعات الحكومية المصرية بدورات عن الإفصاح عن الاختراقات السيبرانية، وطرق الإفصاح الملائم عن إدارة مخاطر الأمن السيبراني، ومعايير أمن تكنولوجيا المعلومات.

- قيام الجامعات المصرية بتطوير المقررات في مرحلة الدراسات العليا بحيث تهتم بتحليل الاختراقات السيبرانية بالإفصاحات عنها، وطرق الافصاح عن إدارة مخاطر الأمن السيبراني (خاصة في القطاع المالي).

٣/٧/٦- مجالات البحث المقترحة:

بناء على نتائج البحث النظرية والعملية، يرى الباحث وجود العديد من المجالات التي يمكن أن تشكل فرصاً لبحوث مستقبلية، ومن أهمها:

-أثر وجود توكيد خارجي مستقل على الإفصاحات عن إدارة مخاطر الأمن السيبراني على العلاقة بين الافصاح عن الاختراقات السيبرانية، وقرار الاستثمار في الشركات.

-أُثر الإفصاحات عن تنوع اعضاء مجلس الإدارة على الإفصاحات عن الاختراقات السيبرانية في الشركات المصرية

- أثر تفاعل جوانب القصور الداخلية والخارجية على الإفصاح عن الاختراقات السيبرانية.

- دور تكرار الإفصاحات عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني على الثقة في تلك الإفصاحات والاستثمار في الشركات التي تعرضت للاختراقات السيبرانية.

- أثر اختلاف القطاع الصناعي على جودة الإفصاحات عن الاختراقات السيبرانية وإدارة مخاطر الأمن السيبراني.

- دور خبرة وعمر إدارة مخاطر الأمن السيبراني في تخفيض الأثر السلبي للإفصاح عن الاختراقات السيبرانية.

المراجع:

المراجع باللغة العربية:

- البنك المركزي المصري (٢٠٢٣)، *مركز الاستجابة للإبلاغ عن حوادث الأمن السيبراني*، جمهورية مصر العربية
https://www.cbe.org.eg/ar/cybersecurity/report-an-incident
-المجلس الأعلى للأمن السيبراني (٢٠١٧)، *الاستراتيجية الوطنية للأمن السيبراني* (٢٠٢١-٢٠١٧)- رئاسة مجلس الوزراء، جمهورية مصر العربية، ١-١٩
- الزيود، أحمد محمود (٢٠٢٠)، إدارة مخاطر الأمن السيبراني في البنوك الأردنية. *Millennium Journal of Economic and Administrative Sciences* . ١(١) .٦-١٤.
- القاضي، كريم محمد حافظ توفيق. (٢٠٢٤)، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات الاستثمار في الشركات الصغيرة والمتوسطة الحجم دراسة تجريبية على الشركات المقيدة بالبورصة المصرية. *مجلة الإسكندرية للبحوث المحاسبية*. ٨ (١). ٣٢٣-٣٧٤
- شرف، إبراهيم أحمد إبراهيم. (٢٠٢٣)، أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين- دراسة تجريبية. *مجلة الإسكندرية للبحوث المحاسبية*. ٧(١) ٢١١-٢٨٢.
- علي، محمود أحمد أحمد، وعلي، صالح علي صالح (٢٠٢٢)، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية. *مجلة الإسكندرية للبحوث المحاسبية*. قسم المحاسبة والمراجعة. ٦(٣) – سبتمبر-١-٤٨
- كعموش، شريف علي خميس ابراهيم (٢٠٢٤)، أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية، *مجلة البحوث المحاسبية*، المجلد ١١ (٣) ، ٩٠٠-٩٨٩

- يوسف، أماني أحمد وهبة، (٢٠٢٢)، واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة: دراسة تطبيقية، *المجلة العلمية للدراسات التجارية والبيئية*، كلية التجارة – جامعة الأزهر، المجلد ١٣ (٢)، ٢٨-١٠٩

المراجع باللغة الانجليزية:

Abukari K., Dutta S., Li,C, Songlian Tang, and Zhu P.,(2024),Corporate communication and likelihood of data breaches, *International Review of economics & Finance*, Volume 94,
103433.

- Alina, C. M., Cerasela, S. E., and Gabriela, G. (2017). Internal audit role in cybersecurity. *Ovidius University Annals, Series Economic Sciences*, 17(2), 510513.
- American Institute of Certified Public Accountants. AICPA. (2017a). *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, AICPA Assurance Services Executive Committee, New York, NY
- American Institute of Certified Public Accountants. AICPA. (2017b). *SOC for Cybersecurity: A Backgrounder*. AICPA, New York, NY

-American Institution of Certified Public Accountants. AICPA. (2018). *Cybersecurity risk management reporting*. Cybersecurity Risk Management Reporting Fact Sheet (aicpa.org)

-Andrew, J., Baker M., and Huang C., 2023.Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play? *Critical Perspectives on Accounting*,9(January), Article 102396

- Asakpa S. T. (2023). From Risk to Resilience: Strengthening Cyber security in Financial Institutions. *International Journal of Advance Research*, Ideas and Innovations in Technology, 9(6).137-145

-Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., and Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, 24(2), 2677-2690.

-Balafoutas, L, S. Czermak, M. Eulerich and H. Fonwagner. (2020). Incentives for Dishonesty: an experimental study with internal auditors. *Economic Inquiry*.Vol.58. Issue.2.764-779

- Berkman, H., Jona, J., Lee, G., and Soderstorm, N., (2018). Cybersecurity Awareness and Market Valuations, *Journal of Accounting and Public Policy*, 37 :508-526.

-Boolaky, P. K., and R. Quick. 2016. Bank directors' perceptions of expanded auditor's reports. *International Journal of Auditing*, 20(2): 158-174.

-Caldarulo M., Welch E. W, and Feeney, M.K., (2022). Determinants of cyber-incidents among small and medium US cities, *Government Information Quarterly*, 39(3),101703

- Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199-224.

- Cheng, X., Hsu, C., and Wang, T. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. *Communications of the Association for Information Systems*, 50(26), 481-500.

- Committee of Sponsoring Organizations of the Tredway Commission (COSO).(2017) E*nterprise Risk Management: Integrating with Strategy and Performance.* Washington, DC

-D'Arcy, J. and Basoglu, K. A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems.* 23(3): 779-805.

- De Arroyabe F., I., and De Arroyabe F., J. C. (2021). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, 17(3). 1-27

-Demek, K. C., and Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems*, 49, 100616.https://doi.org/10.1016/j.accinf.2023.100616

- Fotis, F. (2024). Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis. *Procedia Computer Science*, *251*, 471-478.

-Furnell, S., and Dowling, S. (2019). Cybercrime: a portrait of the landscape. Journal of Criminological Research, *Policy and Practice*. 5. 10.1108/JCRPP-07-2018-0021.

-Gao, L., Calderon ,T. G., and Tang, F. (2020).Public companies' cybersecurity risk disclosures, *International Journal of Accounting Information Systems* ,38,100468.

-GAO. (2016). *Agencies Need to Improve Controls over Selected High-Impact Systems*.

-Goel, S. and Shawky, H. A. 2023. *E*stimating the market impact of security breach announcements on firm values. *Information and Management.* 46(7): 404-410.

-Guo, X., and Fluharty, A. (2024). Mandatory Disclosure of Negative Events and Auditor Behavior: Evidence from a Natural Experiment. *Journal of Risk Financial Managemen*t. 17(11), 497. https://doi.org/10.3390/jrfm17110497.

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

- Jeyaraj A., Zadeh A. and Sethi V. (2021) Cybersecurity Threats and Organizational Response: Textual Analysis and Panel Regression, *Journal of Business Analytics*,4:1, 26-39, DOI: 10.1080/2573234X.2020.1863750
- Jiang, W., Legoria, J., Reichelt, K. J. and Walton, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems*. 36 (1): 151-180.
-Kelton, A. S. (2021). How to reduce the cybersecurity breach contagion effect? . *Current Issues in Auditing*. 15 (2): 1-9.
- ————————————., and Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems*. 34(3): 133-157. https://doi.org/10.2308/isys-52628
-Klemash, S. W., Smith, J. C. and Seets, C. (2020). What companies are disclosing about cybersecurity risk and oversight. *Harvard Law School Forum on Corporate Governance.* August. 2020. https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/
-Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671.
- Li, Y., and Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 7, pp. 8176–8186
-Manoj, K. S. (2021). Banks' holistic approach to cyber security: tools to mitigate cyber risk. *Technology*, *12*(1), 902-910.
- Mazumder M. M. M., and Hossain. D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*, 13 (2), 2023, 217-239
- Mazzoccoli, A. (2023). Optimal Cyber Security Investment in a Mixed Risk Management Framework: Examining the Role of Cyber Insurance and Expenditure Analysis. *Risks*, *11*(9), 154.
- Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*. 11 (101): 1-22. https://doi.org/10.3390/risks11060101
-Ramírez, M.; Rodríguez Ariza, L.; Gómez Miranda, M.E., and Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for Cybersecurity. Disclosure Index. *Sustainability*, *14*, 1390.
- Romanosky S. and Sayers E. L. P. (2024). Enterprise risk management: how do firms integrate cyber risk? .*Management Research Review*. 47 (1). 1-17
-Santhosh,T . , and Thiyagu K (2022) Cyber Safety and Security Awareness Initiatives in India-A Systematic Review – *Indian Manager's Journal of Educational Technology*, 19(1).42-50

Sari, L., Adam, M., and Fuadah, L. L. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. *KnE Social Sciences*, 387-398.

- Security Exchange Commission. SEC (2017), Statement on Cybersecurity, Sept. 20.

-SEC (Securities and Exchange Commission). 2018. Commission statement and guidance on public company cybersecurity disclosures.
https://www.sec.gov/files/rules/interp/2018/33-10459.pdf

-Smaili N., Radu C., and Khalili A.(2023) Board effectiveness and cybersecurity disclosure, *Journal of Management and Governance*. 27:1049–1071

-Srinivas S. and Huigang L., (2022) Being digital to being vulnerable: does digital transformation allure a data breach? *Journal of Electronic Business & Digital Economics*.1 (1/2) 2022. 111-137

- Sundareswaran,V. , Divyalakshm and Poornima (2018), Study OF Cybersecurity in data breaching, *Scientific Journal of Impact Factor*, (5).3.1513-1516

- Tweneboah-Kodua , S , Atsu, F. and Buchanan W. (2018). Impact of cyberattacks on stock performance: a comparative study, *Information & Computer Security*, 26 (5) 2018 pp. 637-652

- Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computer Security*. 38, pp. 97–102. DOI: 10.1016/j.cose.2013.04.004.

- Yang, L., Lau, L., and Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, *28*(1), 167-183