مجلة البحوث المحاسبية

https://com.tanta.edu.eg/abj-journals.aspx

أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية

السادة: شريف علي خميس ابراهيم كعموش

أستاذ مشارك، قسم المحاسبة، كلية الاعمال، جامعه الاسكندرية، مصر

تاريخ النشر الالكتروني: سبتمبر- 2024

للتأصيل المرجعي: كعموش ، شريف علي خميس ابراهيم. **أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية**

، مجلة البحوث المحاسبية ، المجلد 11 (3)،

المعرف الرقمي: 10.21608.2024.37593610/abj

للتواصل مع المؤلف: Sherifkhamiss@gmail.com

أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية

شريف علي خميس ابراهيم كعموش

أستاذ مشارك ،قسم المحاسبة،كلية الاعمال ، جامعه الاسكندرية ،مصر

تاريخ المقال

تم استلامه في30 يوليو 2024، وتم قبوله في20 اغسطس 2024، هو متاح على الإنترنت سبتمبر2024

المستخلص:

استهدف البحث دراسة واختبار أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام كل من العملاء والمستثمرين في الأسهم، كذلك اختبار الأثر المُعَدِل لبعض الخصائص الديموغرافية (الجنس والعمر) على تلك العلاقة، وذلك من خلال دراسة تجريبية على عينة من المحللين الماليين ومديري الاستثمار كاختبار أساسي، ثم استخدام عينة أخرى من الأكاديميين كتحليل حساسية. حيث تم اختبار تأثير بديلين للإفصاح عن إدارة المخاطر السيبرانية وهما؛ الإفصاح من خلال تقرير مجلس الإدارة، والإفصاح في تقرير منفصل.

وتوصلت النتائج الاختبارات الأساسية على مستوى المحللين الماليين ومديري الاستثمار إلى أن كل من بديلي الإفصاح له تأثير معنوي على أحكام المستثمرين في الأسهم (والمتمثلة في تقييم السهم وقرار الاستثمار) وقرارات العملاء (والمتمثلة في التعامل على الخدمات الالكترونية للبنك واستخدام بطاقات الائتمان للشراء عبر الانترنت). كما أن الإفصاح من خلال تقرير منفصل كان له تأثير أكثر معنوية على أحكام المستثمرين مقارنة بالإفصاح من خلال تقرير مجلس الإدارة. غير أنه لم يكن هناك فرق معنوي بين بديلي الإفصاح بخصوص قرارات العملاء. كما أشارت النتائج إلى اختلاف النتائج السابقة باختلاف جنس المستخدمين وبديل الإفصاح، حيث جاء تأثير الإفصاح من خلال تقرير مجلس الإدارة معنوي على أحكام المستثمرين الذكور فقط دون الإناث، ومعنوياً على قرارات العملاء الذكور والإناث، بينما تأثير الإفصاح من خلال تقرير منفصل معنوياً على أحكام المستثمرين الذكور والإناث، بينما كان معنوياً على قرارات العملاء الذكور فقط. كما أشارت النتائج إلى اختلاف النتائج السابقة باختلاف عمر المستخدمين وباختلاف بديل الإفصاح، حيث جاء تأثير الإفصاح من خلال تقرير مجلس الإدارة معنوي على أحكام المستثمرين وكذلك العملاء الأكبر سناً فقط دون الأصغر سناً، بينما تأثير الإفصاح من خلال تقرير منفصل معنوياً على أحكام المستثمرين والعملاء الأكبر والأصغر سناً.

وفيما يتعلق بالاختبارات على الأكاديميين كتحليل حساسية، فقد أشارت النتائج إلى أن بديلي الإفصاح كان لهما تأثيراً معنوياً على قرارات العملاء فقط، بينما الإفصاح فقط من خلال تقرير منفصل كان له تأثيراً معنوياً على قرارات المستثمرين. كما لم يكن للجنس أثراً معدلاً لتلك النتائج، بينما كان هناك اختلاف بالنتائج باختلاف العمر

الكلمات المفتاحية: الإفصاح عن الأمن السيبراني؛أثر بدائل الإفصاح؛ إدارة مخاطر الأمن السيبراني؛ الأمن السيبراني في البنوك

Abstract

The study aimed to test the effect of banks' disclosure alternatives about cybersecurity risk management on the judgments of both clients and stock investors, as well as to test the moderating effect of some demographic characteristics (gender and age). A designed experimental study is used on a sample of financial analysts and investment managers as a primary test, and then using another sample of academics as a sensitivity analysis. Two alternatives to cybersecurity risk management disclosure was tested: disclosure through a board of directors' report, and disclosure in a separate report. The results of the primary tests on financial analysts and investment managers concluded that both disclosure alternatives have a significant effect on the judgments of stock investors (stock valuation and investment decision) and clients' decisions (using E-banking and using credit cards to purchase online). Disclosure through a separate report has more significant effect on investor judgments compared to disclosure through a BOD report. However, there was no significant difference between the two disclosure alternatives regarding clients' decisions. The results also indicated that the previous results differed according to the gender, as the effect of disclosure through the BOD report was significant on the judgments of male investors only, but not females, and significant on the decisions of male and female clients, while the effect of disclosure through a separate report was significant on the investors' judgments of male and female, while it was significant on the clients' decisions of male only. The results also indicated that the previous results differed according to age, as the effect of disclosure through the board of directors' report was significant on the judgments of elder investors and clients only, but not younger, while the effect of disclosure through a separate report was significant on the old and young investors and clients' judgments.

With regard to academics as a sensitivity analysis, the results indicated that the two disclosure alternatives had a significant effect on clients' decisions only, while disclosure through a separate report only had a significant effect on investors' decisions. Gender did not have a moderating effect on these results, while there was a moderating effect of age.

Keywords : Cyber security disclosure; Disclosure alternatives effect; cybersecurity risk management; cyber security in banks;

1- مقدمة البحث:

أدى التطور المتسارع في مجال تكنولوجيا المعلومات واستخدامها في عمليات الشركات إلى تعرض تلك الشركات بشكل متزايد لمخاطر الأمن السيبراني. وأصبح لدى المتعاملين مع تلك الشركات حالة من عدم التأكد بشأن أمن المعلومات والعمليات، ما قد يقدم دافعاً لدى الشركات لتقديم المزيد من الإفصاح عن تلك المخاطر السيبرانية وكيفية إدارتها، للحد من عدم تماثل المعلومات المتعلق بإجراءات وسياسات إدارتها لمخاطر الأمن السيبراني (Jaing et al., 2022).

وعلى مستوى المؤسسات المالية، فقد ظهرت أهمية الأمن السيبراني، وضرورة تجنب المخاطر التي تهدد الأمن السيبراني مع القدرة على التعامل مع أثارها ومعالجتها في الوقت المناسب، حيث تنعكس تلك المخاطر سلباً على الاستقرار المالي لهذا القطاع، وتهدد عملياته والمتعاملين معه، وقد أيدت تقارير البنك الدولي أن القطاع المالي يعد من أكثر القطاعات التي تتعرض لاختراقات الأمن السيبراني، حيث جاءت تقديرات البنك الدولي بأن خسائر القطاع المالي تمثل 65% من القطاعات الأخرى عام 2017 (صندوق النقد العربي 2019)، وأن تلك الهجمات تضاعفت 4 مرات من عام 2017 إلى وقت إعداد التقرير الأخير عام 2024، الأمر الذي يتطلب وضع استراتيجيات على مستوى البنوك المركزية للتعامل مع تلك المخاطر المتزايدة (IMF, 2024)، كذلك الحاجة إلى اتباع منهج منظم لإدارة تلك المخاطر على مستوى البنك، وهو ما يعد أمراً حيوياً للبنوك والمتعاملين معها والمستثمرين (Zbar, 2022; Ali et al., 2022).

وفي مصر فقد اهتم البنك المركزي بحماية الأمن السيبراني في القطاع المصرفي ووضع أهداف الامن السيبراني لحماية أصول المؤسسات المالية ومواردها، من خلال العمل على تقليل احتمالات ظهور أي تهديد والحد من الأضرار الناجمة عنه، وضمان رجوع العمليات العادية إلى حالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني. كما أنشأ البنك المركزي أول مركز قطاعي في مصر للاستجابة لطوارئ الحاسب الآلي للقطاع المالي، وأصدر إطار الأمن السيبراني التنظيمي، لتعزيز مواصلة سياسات التقييم الذاتي، والمساعدة في الحفاظ على بيئة عمل وبنية تحتية تتمتع بأعلى درجات الأمن والحماية للبيانات والمعلومات.

ونتيجة لأهمية المخاطر السيبرانية التي تتعرض لها الشركات بصفة عامة، والبنوك بصفة خاصة، وما تتبناه هذه الشركات من استراتيجيات لإدارة تلك المخاطر، فمن المتوقع أن يكون لدى المتعاملين مع ذلك القطاع الحيوي طلباً متزايداً على الإفصاح حول تلك المخاطر السيبرانية، وما إذا كانت البنوك لديها القدرة على إدارتها والتعامل معها والحد من آثارها إذا ما وقعت. وهو ما دعا العديد من الدراسات لاختبار أثر الإفصاح عن تلك المعلومات على أحكام وقرارات المستفيدين (علي وعلي، 2021؛ يوسف 2022؛ الرشيدي وناصر، 2019؛ شرف، 2023؛ Frank et al. 2019; Yang et al. 2020)، إلا أن تلك الدراسات لم تأخذ في الاعتبار بدائل ذلك الإفصاح ومحتواه، الأمر الذي يتطلب البحث حول تأثير بدائل ذلك الإفصاح. وبالتالي تستهدف الدراسة أختبار أثر بدائل

الإفصاح عن إدارة مخاطر الأمن السيبراني في القطاع المصرفي على أحكام المستفيدين، حيث امتدت الدراسة لاختبار الأثر على أحكام المستثمرين، وعملاء البنوك باعتبارهما من أهم الفئات المستفيدة (أصحاب المصالح) من البنوك. فوفقاً لنظرية أصحاب المصالح، فإن أصحاب المصلحة بالبنوك على وجه التحديد يمثلون مجموعة أوسع من مستخدمي المساهمين (مثل العملاء)، وبالتالي فإن الشركات مطالبة بأن تكون أكثر شفافية تجاه أصحاب المصلحة فيما يتعلق بالإفصاح عن إدارة المخاطر السيبرانية، بما يبني الثقة لدى المتعاملين (Klemash et al. 2020) ويحد من مخاطر التقاضي ومن عدم التأكد الذي يمكن أن يؤدي إلى خسارة العملاء (Jaing et al., 2022).

وقد تناولت العديد من الدراسات أُثر الخصائص الديموغرافية لأصحاب المصالح على قراراتهم، لاسيما العمر والجنس، سواء تقييم الأسهم والاستثمار كمستثمرين (Niessen and Zimmerer, 2024; Shaikh et al. 2019; Shah, 2023; Siraji et al. 2021; Jain and Mandot, 2021)، أو قرارات التعامل مع الخدمات الالكترونية للبنوك والتعامل المصرفي عبر الانترنت كعملاء للبنك (Elena-Bucea et al. 2021; Yuen, 2013; محمد ، 2021)، وبالتالي يتطلب الأمر دراسة الأثر المعدل لتلك العوامل على قرارات أصحاب المصالح.

2- مشكلة البحث:

اهتمت العديد من الدراسات باختبار أثر الإفصاح عن معلومات إدارة مخاطر الأمن السيبراني على أحكام وقرارات أصحاب المصالح (علي وعلي، 2021؛ يوسف، 2022؛ الرشيدي وناصر، 2019؛ شرف، 2023؛ Goel and Shawky, 2023; Frank et al., 2019; Yang et al., 2020). إلا أن تلك الدراسات لم تأخذ في الاعتبار بدائل ذلك الإفصاح ومحتواه، وذلك على الرغم من أن بعض الدراسات السابقة أشارت إلى أن اختلاف شكل عرض المعلومات قد يكون له تأثير مختلف على قرارات المستخدمين، وأن الإفصاح عن ذات المعلومات قد يكون لها آثار مختلفة على المستثمرين إذا ما تم عرضها بطرق مختلفة وتم تفسير ذلك من خلال نظريتين هما **نظرية التوافق الإدراكي** Cognitive Fit **ونظرية الإدراك المحدود** Limited Attention (Kelton et al., 2010; Hishleifer and Teoh, 2003). وبالتالي يتطلب الأمر البحث حول تأثير بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني، على أحكام أصحاب المصالح.

فضلاً عن أن الدراسات السابقة لم تركز على القطاع المالي والبنوك على الرغم من أن ذلك القطاع يعد أحد أهم القطاعات المعنية بالمخاطر السيبرانية وإدارتها (IMF, 2024; McKinsey, 2024; Firoozi and Mohsni, 2023;) ، وبالتالي تسعى الدراسة الحالية لسد هذه الفجوة البحثية.

وعلى جانب أخر اهتمت الدراسات السابقة باختبار أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على قرارات وأحكام المستثمرين، غير أنه ووفقاً لنظرية أصحاب المصالح فإن الشركات مطالبة بأن تكون أكثر شفافية تجاه كافة أصحاب المصلحة وليس فقط امستثمرين، وتفترض نظرية أصحاب المصلحة أن الحفاظ على الثقة المتبادلة والتعاون مع جميع أصحاب المصلحة هو استراتيجية عمل تقلل من تكاليف التعاقد والتي تشمل

الدعاوى القضائية التي يرفعها أصحاب المصلحة نتيجة لانتهاك الأمن السيبراني، ويحد من عدم التأكد الذي يمكن أن يؤدي إلى خسارة العملاء (Jaing et. al., 2022). ولعل العملاء هم من أهم الفئات التي تتعامل مع البنوك، إذ أنهم المصدر الرئيسي للتمويل، والمصدر الرئيسي لتحقيق الإيرادات. فبمراجعة القوائم المالية لبعض البنوك المقيدة بالبورصة المصرية وجد الباحث أن ودائع العملاء تمثل في المتوسط 93% من إجمالي الالتزامات، وتمثل 89% من إجمالي الالتزامات وحقوق الملكية. لذلك، يمكن أن يقدم الإفصاح عن إدارة المخاطر السيبرانية معلومات قد تساعد العملاء في تقييم المخاطر الحالية والمستقبلية الناجمة عن حدوث الاختراق وما إذا كانوا سيواصلون علاقتهم مع البنك.

ويمكن صياغة مشكلة البحث في الإجابة على التساؤل الآتي عملياً في مصر:

هل تؤثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على قرارات عملاء البنك وأحكام المستثمرين في أسهمه؟ وهل تتأثر تلك العلاقة باختلاف بعض الخصائص الديموغرافية لهم؟

3- هدف البحث:

يهدف البحث إلى دراسة واختبار أثر بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام كل من المستثمرين والعملاء بالبنوك. كما يهدف البحث إلى اختبار الأثر المعدل لكل من عاملي الجنس والعمر لكليهما، وذلك من خلال دراسة تجريبية.

4- أهمية ودوافع البحث:

تنبع أهمية الدراسة من الموضوع الذي تتناوله وهو ما يرتبط بالأمن السيبراني في المؤسسات المالية خاصة البنوك، ومدى قدرة البنوك على الالتزام بالاستراتيجية الوطنية للأمن السيبراني من خلال إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على أحكام المستفيدين الرئيسيين بالبنوك (المساهمين والعملاء).

وفي سياق **الأهمية العلمية والبحثية**، فعلى الرغم من اهتمام الأدب المحاسبي في الفترة الأخيرة بأثر الإفصاح عن مخاطر الأمن السيبراني، غير أن التركيز كان حول أثر الإفصاح عن تعرض الشركات لهجمات سيبرانية على قيمة الشركة، إلا أن القليل جدا من الدراسات تناول أثر الإفصاح عن إدارة مخاطر الأمن السيبرانى وما تقوم به الشركات بهدف تجنب تلك الخاطر ومعالجة آثار وقوعها بصورة سريعة، فضلاً عن ذلك فإن الباحث لم يجد دراسات تناولت الأثر التفاضلي لبدائل الإفصاح عن إدارة مخاطر الأمن السيبراني بالبنوك، كما لم يجد دراسات سابقة تناولت أثر الإفصاح عن القضايا المرتبطة بالأمن السيبراني على عملاء البنوك على الرغم من أهمية تلك الفئة كمقدمي تمويل من جهة ومصدر رئيسي للإيرادات للبنوك من جهة أخرى.

وفي مجال **الأهمية العملية**، فإن البحث يفتح مجالاً هاماً يتعلق ببدائل الإفصاح عن إدارة مخاطر الأمن السيبراني وتأثيرها على المتعاملين مع البنوك، وبالتالي يمكن أن يسهم البحث في تقديم رؤية حول أفضلية بدائل الإفصاح

التي يمكن اتباعها لتقديم معلومات بشأن إدارة مخاطر الأمن السيبراني لفئات المستفيدين الأساسيين التي تهتم بها البنوك.

كما يكتسب البحث **أهميته للجهات التنظيمية وواضعي المعايير**، من خلال ما يمكن أن يسهم به في تقديم رؤية للجهات التنظيمية، وواضعي المعايير، حول أهمية الإفصاح عن إدارة مخاطر الأمن السبراني، وبدائل الإفصاح الأكثر تأثيراً على المستفيدين، بما يمكن أن يسهم في تقديم مساهمة كخطوة أولى لتنظيم ذلك الإفصاح وإيجاد الإطار الملائم له.

وأخيراً تبرز **الأهمية المتعلقة بالقطاع المصرفي**، لما يمكن أن تسهم به إدارة المخاطر السيبرانية واستجابة المستفيدين لتلك الممارسات، من تحقيق الاستقرار المالي للبنوك، وهو أحد أهم الأهداف على مستوى القطاع المصرفي وهو ما ينعكس على الإقتصاد العام للدولة.

5- حدود الدراسة

- تقتصر المتغيرات المعدلة محل الدراسة على كل من الجنس والعمر، على الرغم من وجود خصائص ديموغرافية أخرى قدمتها الدراسات السابقة يمكن أن يكون لها تأثير على قرارات المستثمرين، وقرارات العملاء بالتعامل على الخدمات الالكترونية للبنك. إضافة إلى عوامل أخرى غير ديموغرافية قد تؤثر على قرارات الاستثمار وقرارات التعامل على الخدمات الالكترونية للبنوك قدمتها الدراسات السابقة.
- يتحدد نطاق البحث بأثر بدائل الإفصاح على إدارة مخاطر الأمن السيبراني على أحكام المستفيدين بالتركيز على فئتين رئيسيتين وهما المستثمرين، والعملاء، وبالتالي يخرج عن نطاق الاختبار التجريبي للبحث الأثر على الفئات الأخرى من المستفيدين، كما يخرج عن نطاق البحث أثر الإفصاح عن المخاطر الفعلية (الاختراقات التي حدثت) على أحكام المستفيدين.
- على الرغم من إمكانية وجود أكثر من بديل يمكن استخدامه للإفصاح عن إدارة مخاطر الأمن السيبراني، (مثل تقارير الحوكمة والاستدامة، أوضمن تقرير مجلس الإدارة، أو نماذج تتطلبها البورصة على غرار ما تتطلبه البورصة الأمريكية للافصاح عن الأمن السيبراني ضمن تقارير الـ K-10، أو في تقرير منفصل على غرار التقرير الذي قدمته جمعية المحاسبين القانونيين الأمريكية AICPA)، إلا أن البحث يركز على طريقتين فقط وهما الإفصاح من خلال تقرير مجلس الإدارة، أو من خلال تقرير مستقل وفقاً لما تبنته AICPA.

6- منهجية الدراسة:

لتحقيق هدف البحث والاجابة على تساؤلاته يعتمد الباحث على دراسة نظرية وأخرى تجريبية، حيث تعتمد الدراسة النظرية على تحليل وتقييم الدراسات السابقة بهدف التأصيل النظري لمفهوم إدارة المخاطر السيبرانية وأهميته، وأثاره، والإفصاح عنه، مع محاولة التركيز على القطاع المصرفي، إضافة إلى الوقوف على الفجوة البحثية وتطوير واشتقاق فروض الدراسة. ثم ينتقل البحث في شقه التطبيقي لاختبار فروض

الدراسة وذلك من خلال دراسة تجريبية على عينة من المحللين الماليين ومديري الاستثمار بمصر، مع تحليل حساسية بالتطبيق على عينة من الأكاديميين وأعضاء هيئة التدريس. حيث يمر المشاركون في الحالة التجريبية بمرحلتين، يقدم لهم في المرحلة الأولى قوائم مالية ذات تقرير مراجعة غير معدل، ويطلب منهم الإجابة عن بعض الأسئلة وتقديم أحكامهم المهنية فيما يتعلق بتوقعاتهم بشأن سعر السهم واتخاذ قرار الاستثمار في الشركة محل الدراسة كمستثمرين، ثم يطلب منهم اتخاذ قرار بشأن التعامل مع الخدمات الالكترونية للبنك واستخدام بطاقاته الائتمانية للشراء عبر الانترنت كعملاء. ثم يقدم لهم في المرحلة الثانية إفصاحاً عن إدارة مخاطر الأمن السيبراني من خلال بديلين للإفصاح؛ البديل الأول من خلال تقرير مجلس الإدارة يقدم للمجموعة التجريبية الأولى، والبديل الثاني من خلال تقرير منفصل خاص بإدارة الأمن السيبراني يقدم للمجموعة الثانية، ويُطلب من المشاركين في ضوء المعلومات الجديدة الإجابة على التساؤلات الخاصة بتقديرهم لسعر السهم وقرار الاستثمار كمستثمرين، وقرار التعامل مع الخدمات الالكترونية للبنك واستخدام بطاقاته الائتمانية للشراء عبر الانترنت كعملاء. ويقدم القسم (11-3) وصفاً للحالة التجريبية واجراءاتها ومميزات التصميم التجريبي المستخدم في الدراسة.

7- خطة البحث:

تحقيقاً لهدف البحث وفي ضوء حوده، يتم تقسيم البحث إلى المحاور التالية

8- إدارة مخاطر الأمن السيبراني- من منظور تقني ومحاسبي

8-1 مفهوم وأنواع الخطر السيبراني

8-2 إدارة مخاطر الأمن السيبراني

8-3 أهمية إدارة الأمن السيبراني في البنوك وغيرها من المؤسسات المالية

8-4 الوضع في مصر فيما يتعلق بإدارة المخاطر السيبرانية في القطاع المصرفي

9- الإفصاح عن إدارة مخاطر الأمن السيبراني من منظور المحاسبة المالية

10- فروض الدراسة

11- الدراسة التجريبية والاختبارات الاحصائية

12- نتائج الدراسة والتوصيات ومجالات البحث المقترحة

8- إدارة مخاطر الأمن السيبراني- من منظور تقني ومحاسبي

مع التوسع في الاستخدام المكثف للتكنولوجيا الرقمية والطبيعة المتطورة للأصول الرقمية، زادت حالات اختراقات أمن المعلومات والشبكات والعمليات الرقمية، وأصبحت المخاطر الأمنية مثل تسرب البيانات، والهجمات على الشبكات، والفجوة الرقمية، موضع اهتمام واسع النطاق وأصبحت تدريجياً تمثل عاملاً عائقاً لا يمكن تجاهله سواء على مستوى الاقتصاد الكلي والحكومات الرقمية (Wang et al., 2023)، أو على المستوى السياسي والأمن

القومي (Sevilla, 2021)، أو على مستوى الشركات ومنشآت الأعمال والتي قد يؤدي تعرضها لهذا الخطر إلى تآكل قدرتها التنافسية، والأثر السلبي على سمعتها وقدراتها التشغيلية مما يهدد بخسارة العملاء (D'Arcy and Basoglu, 2022; Dodla and Jones, 2023; Ali et al., 2022)، وبالتالي يمكن القول بأن الأمن السيبراني له العديد من الأبعاد سواء الإقتصادية، أو العسكرية، والاجتماعية، والسياسية والقانونية (البغدادي، 2021).

في دراسة أجرتها شركة Proofpoint مع معهد Ponemon[1] عام 2023 على الأمن السيبراني، قام المعهد باستطلاع رأي 653 من ممارسي تكنولوجيا المعلومات وأمن تكنولوجيا المعلومات بالقطاع الصحي. وجاءت بعض نتائج التقرير لتشير إلى تعرض 88% من المؤسسات لمتوسط 40 هجوماً خلال الـ 12 شهراً الماضية، وبلغ متوسط تكلفة الهجوم السيبراني ما يقرب من 5 ملايين دولار، أي بزيادة قدرها 13٪ عن العام السابق، كما تعرضت 64% من المؤسسات لهجوم على سلسلة التوريد خلال العامين الماضيين. ومن بين هذه المجموعة، أشار 77% أن هذه الهجمات أثرت على القدرة التشغيلية للمؤسسات وقدرتها على تقديم الخدمات. كذلك تعرض 63% من المؤسسات لـ 21 اختراقًا سحابياً في المتوسط خلال العامين الماضيين (Proofpoint, 2023).

وفي التقرير الخاص بدراسة تكاليف الاختراقات الأمنية لعام 2023، لمعهد Ponemon برعاية IBM Security[2]، فإن متوسط تكلفة الاختراق على مستوى العالم في عام 2023 بلغت 4.45 مليون دولار لكل اختراق بزيادة قدرها 15% على مدار السنوات الثلاثة السابقين، كما أن متوسط الوفر الذي تحققه الشركات التي تستخدم نظم الذكاء الاصطناعي للأمن السيبراني على نطاق واسع 1.76 مليون دولار مقارنة بالمؤسسات الأخرى. كما أشار التقرير إلى أن 51% من المؤسسات تخطط لزيادة الاستثمارات الأمنية نتيجة للاختراق، بما في ذلك تخطيط واختبار الاستجابة للحوادث (IR)، وتدريب الموظفين، وأدوات الكشف عن التهديدات والاستجابة لها. ووفقاً لتلك الدراسة التي تمت على 17 صناعة وقطاع من 16 دولة، فقد جاءت دول الشرق الأوسط في المركز الثاني لتكلفة الخروقات الأمنية بعد الولايات المتحدة، وبلغ معدل زيادة تكلفة الخروقات لدول الشرق الأوسط 8.2% لعام 2023 مقارنة بعام 2022. كما جاء القطاع الصحي يليه القطاع المالي على رأس القطاعات التي تعرض لتكلفة الاختراقات خلال العام 2023 (IBM, 2023).

أما على مستوى القطاع المالي، فقد أشار تقرير لصندوق النقد الدولي أن خسائر المخاطر السيبرانية تضاعفت أربعة أضعاف منذ عام 2017، كما أن القطاع المالي على وجه الخصوص كان عرضة للمخاطر السيبرانية،

(1) تأسس معهد Ponemon في عام 2002، وهو متخصص للبحث المستقل والتعليم ويقوم بإجراء دراسات تجريبية حول القضايا الهامة التي تؤثر على إدارة وأمن المعلومات الحساسة حول الأشخاص والمنظمات.

(2) تعتبر شركة IBM من أكبر المؤسسات العاملة في التكنولوجيا والخدمات اللازمة للمساعدة على حل مشاكل الأعمال المرتبطة بالتكنولوجيا وأمن المعلومات.

وكانت البنوك هي الأكثر عرضة لتلك الهجمات. كما أن الحوادث التي يتعرض لها القطاع المالي قد تؤدي إلى تهديد الاستقرار المالي والاقتصادي إذا ما أدت إلى تآكل الثقة في النظام المالي، أو تعطيل الخدمات الضرورية، ولا شك أن ذلك يتطلب وضع استراتيجيات وطنية كافية لحماية الأمن السيبراني، مصحوبة بأطر تنظيمية وقدرات رقابية فعالية، بما يضمن تعزيز قوة القطاع المالي (IMF, 2024).

1-8 مفهوم وأنواع الخطر السيبراني:

بصفة عامة لا يوجد تعريف نمطي للخطر السبراني (Gatzert and Schubert, 2022)، غير أن دراسة Gains et al. (2022) ترى أن التعريف الأكثر شمولاً لمخاطر الأمن السيبراني، هو الصادر عن لجنة أنظمة الأمن القومي Committee on National Security Systems (CNSS) حيث تعرفه بأنه " مقياس لمدى تعرض المنشأة للتهديد من خلال ظرف أو حدث محتمل، وعادةً ما يكون دالة في التأثيرات السلبية التي قد تنشأ واحتمالية الحدوث". وترى تلك الدراسة أن المخاطر السيبرانية هي التي تنشأ عن فقدان السرية أو النزاهة أو توفر المعلومات أو أنظمة المعلومات وتعكس التأثيرات السلبية المحتملة على العمليات أو المؤسسات ككل.

كما يعرف التقرير الصادر عن الاتحاد الدولي للاتصالات ITU الجريمة السيبرانية بأنها "أعمال إجرامية تُرتكب داخل أو عن طريق شبكات الكمبيوتر، أو ضدها" (ITU, 2010-2011). وتعرف دراسة فريد (2022) مخاطر الأمن السيبراني بأنها المخاطر التي تهدد عمليات الشركة بما في ذلك رؤية الشركة أو رسالتها أو إدارتها أو صورتها أو سمعتها أو أصولها أوأفرادها بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات أو نظم المعلومات والشبكات. بينما ترى دراسة Gatzert and Schubert (2022) أنه يمكن النظر للمخاطر السيبرانية كفئة فرعية من مخاطر التشغيل، حيث يمكن تعريفها بأنها المخاطر التشغيلية لأصول المعلومات والتكنولوجيا التي قد تؤثر على سرية أو توافر أو سلامة المعلومات أو نظم المعلومات. أما دراسة Melaku (2023) فترى أن الخطر السيبراني يمثل احتمالات التأثير السلبي على المعلومات الحساسة والعمليات التجارية للمؤسسة.

ويمكن القول بأن المخاطر السيبرانية تمثل التهديدات التي قد تحدث لنظام تكنولوجيا المعلومات بشكل يجعله غير قادر على أداء وظائفه بصورة كاملة، وقد تتضمن مخاطر الأمن السيبراني إما التهديد لقدرة النظام في توفير حماية المعلومات والسرية المرتبطة بالمتعاملين، أو تحريف العمليات بحيث تتم المعالجات بشكل غير صحيح. وتواجه الشركات تحديات متطورة تتعلق بالأمن السيبراني والتي يستخدم فيها المهاجمون مجموعة معقدة من الوسائل مثل استخدام بيانات اعتماد الوصول المسروقة، والبرامج الضارة وبرامج الفدية والتصيد الاحتيالي وهجمات حجب الخدمة المقدمة إلى غير ذلك من الطرق (SEC, 2018)

ويرى البغدادي (2021) أنه يمكن النظر لمخاطر الأمن السيبراني باعتبارها مرتبطة بالفضاء السيبراني من محورين؛ الأول يتمثل في **المحور الاقتصادي** والذي ينقسم إلى مجال يتعلق بصناعة تكنولوجيا المعلومات والبرمجيات والاتصالات والذي يغطي صناعة الشبكات والبرمجيات والأجهزة والخدمات الأخرى، ومجال التجارة الالكترونية؛ بينما يتمثل **المحور الثاني** في أمن المعلومات، والقدرة على اختراق أمن الأنظمة والوصول غير المصرح به.

ويرى شحاته (2022) أن هناك مجموعتين من المخاطر المرتبطة باستخدام تكنولوجيا المعلومات، تشمل **الأولى مخاطر الأداء**، والمرتبطة بفشل الأدوات والتقنيات والبنية الأساسية التكنولوجية في تحقيق أهدافها والمهام المنوطة بها، بينما تشمل المجموعة **الثانية مخاطر الأمن السيبراني** والتي تتضمن ثلاث أنواع وهي؛ (أ) **خطر اختراق الحماية المادية**، ويمثل اختراق المكونات المادية للبنية التكنولوجية المعلوماتية للشركة (كالوصول إلى الاقراص المرنة للشركة والأجهزة الخاصة بالشبكات والتي تتضمن أي معلومات أو كلمات سرية يمكن الاعتماد عليها لإتمام عملية الاختراق)؛ (ب) **خطر اختراق الحماية المتعلقة بالعاملين**، وتمثل المخاطر الداخلية والخارجية المتعلقة بسلوك العاملين داخل الشركة، مثل انتهاك التصريح أو قيام العاملين بالشركة باستغلال علاقاتهم ووظائفهم للوصول غير المصرح به للمعلومات؛ (ج) **خطر اختراق الحماية المتعلقة بالمعلومات والاتصالات**، والذي يتضمن هجمات البيانات كالنسخ غير المصرح بها للبيانات، وهجمات البرامج الجاهزة كالفيروسات.

وقد أشارت دراسة Teimoor (2021) إلى أن هناك ثلاثة أنواع من المهاجمين قد يعرضون مستويات حماية قواعد البيانات للخطر وهم؛ (أ) الدخيل Intruder: هو شخص غير مرغوب فيه وليس له صلاحيات على قاعدة البيانات ويحاول الوصول للمعلومات بقاعدة البيانات عن طريق التحايل على نظام الحماية؛ (ب) الداخلي Insider: أحد الأعضاء الموثوق بهم والذي له بعض الصلاحيات للدخول على بعض المعلومات بقاعدة البيانات، غير أنه يقوم بمخالفة الصلاحيات الممنوحة له ويحاول الوصول إلى ما هو أبعد من صلاحياته. (ج) مسؤول النظام Admin: وهو الشخص المسؤول عن تشغيل النظام، والذي قد يخترق حدود إدارته للنظام في سعي منه للتجسس على أنشطة إدارة قاعدة البيانات للحصول على معلومات حساسة.

وترى دراسة Teimoor (2021) أنه يمكن الهجوم على النظام بطريقتين: الهجوم المباشر Direct attack، وتشير إلى الاستهداف المباشر للبيانات المطلوبة، وذلك إذا لم تكن هناك وسائل حماية لقاعدة البيانات، وإذا لم ينجح هذا النوع من الهجوم، ينتقل المهاجم إلى النوع الثاني وهو الهجوم غير المباشر Indirect attack، وفي هذا النوع لا يتم مهاجمة الهدف بشكل صريح، لكن يتم الحصول على البيانات من الهدف بشكل غير مباشر من خلال عناصر أخرى مثل عمل العديد من اقتراحات لاسم المستخدم، استخدام العديد من الاسئلة المختلفة لمحاولة اجتياز آلية المصادقة بالنظام، وهذا النوع من التهديدات يصعب متابعته، كما أوضحت الدراسة أن هجمات قواعد البيانات تتكون من نوعين الهجوم؛ الأول هو **الهجوم السلبي**، حيث يقوم المهاجم بالاطلاع على البيانات وفحصها

دون التعديل على قاعدة البيانات، والثاني هو **الهجوم النشط**، وهو الأكثر خطورة، حيث يتم تعديل قيم قاعدة البيانات أثناء الهجوم.

وبذلك يمكن القول بأن أهداف الهجمات السيبرانية قد تتنوع بشكل كبير، وقد تشمل سرقة البيانات، أو تحريفها، أو تدمير الأصول المالية أو الملكية الفكرية أو غيرها من المعلومات الحساسة للشركة أو عملائها أو شركائها التجاريون، كذلك تعطيل عمليات الشركة والتأثير على قدرتها التشغيلية وتقديم خدماتها بكفاءة (SEC, 2018).

وينتج عن تلك المخاطر أثاراً سلبية على عمليات الشركات والأداء المالي وغير المالي، وتشمل تلك الآثار السلبية؛ (1) تكاليف العلاج نتيجة مسؤولية الشركة عن الأصول أو المعلومات المسروقة والحاجة لدفع تعويضات أو تقديم حوافز للعملاء للمحافظة على العلاقات معهم بعد الهجوم، وإصلاحات الضرر في النظام واستعادة البيانات المفقودة؛ (2) زيادة تكاليف حماية الأمن السيبراني للحاجة إلى المزيد من نظم الحماية والأفراد المُدَربين والاستشاريين؛ (3) الإيرادات المفقودة نتيجة استغلال معلومات الملكية الفكرية والتأثير السلبي على السمعة وخسارة العملاء؛ (4) تكاليف الدعاوي القضائية والمخاطر القانونية والتنظيمية؛ (5) ارتفاع أقساط التأمين؛ (6) زيادة المخاطر التشغيلية واحتمالية توقف الخدمات أو التأثير على كفاءتها؛ ويؤدي كل ما سبق إلى الإضرار بقدرة الشركة التنافسية وسعر السهم، وحقوق المساهمين(D'Arcy and Basoglu, 2022; Janvrin and Wang 2022; SEC,2018).

وقد توصلت دراسة (Zbar, 2022) إلى أنه على الرغم من أن البنوك تتبع العديد من سياسات وإجراءات الحماية الفنية في نظام معلوماتها على مستوى عالي، إلا أنه قد تحدث مخاطر في نظام أمن المعلومات بشكل متكرر نتيجة لقلة الخبرة والوعي والتدريب.

8-2 إدارة مخاطر الأمن السيبراني:

تعرف وكالة الأمن السيبراني الأمريكي ACDA الأمن السيبراني بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي بما يضمن سرية المعلومات وسلامتها وتوافرها"[3]. كما يعرف التقرير الصادر عن الاتحاد الدولي للاتصالات ITU الأمن السيبراني بأنه "مجموعة من الأنشطة التي تتضمن تشكيلة من الأدوات، والسياسات، والضمانات الأمنية، والإرشادات، ومداخل إدارة المخاطر، والتدريب، وأفضل الممارسات، والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمات والمستخدمين" (ITU, 2010-2011). ووفقاً للجنة الأوراق المالية والبورصات الأمريكية (SEC)، يُعَرف الأمن السيبراني بأنه:[4]

([3]) America's Cyber Defense Agency, https://www.cisa.gov/news-events/news/what-cybersecurity

([4]) نقلاً عن: Janvrin and Wang (2022)

"النشاط أو العملية أو القدرة أو الاستطاعة أو الحالة التي بموجبها يمكن حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها من و/أو الدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال".

ومن خلال استخدام النظم الخبيرة لمطابقة التعريفات المختلفة توصلت دراسة Gains et al. (2022) إلى أن تعريف الأمن السيبراني الوارد بالمبادرة الوطنية لوظائف ودراسات الأمن السيبراني National Initiative for Cybersecurity Careers and Studies (NICCS) هو التعريف الأكثر شمولاً، حيث يُعَرف الأمن السيبراني بأنه "الإستراتيجية والسياسة والمعايير المتعلقة بأمن الفضاء الإلكتروني والعمليات فيه، وتشمل مجموعة كاملة من سياسات وأنشطة الحد من التهديدات، والحد من نقاط الضعف، والردع، والمشاركة الدولية والاستجابة للحوادث، والمرونة، والتعافي، بما في ذلك عمليات شبكات الكمبيوتر وضمان المعلومات...". وبالتالي يمكن القول بأن دور الأمن السيبراني لا ينحصر فقط في استراتتيجيات المنع بل يمتد أيضاً إلى تخفيف الأضرار والخسائر التي تحدث في حالة حدوث هجمات سيبرانية، وإصلاح ما أحدثته هذه الهجمات في أسرع وقت.

وقد عرف Alina et al. (2017)[5] إدارة المخاطر السيبرانية بأنه النشاط الذي يؤمن حماية الموارد المرتبطة بتكنولوجيا المعلومات والاتصالات، بما يضمن الحد من الخسائر والأضرار في حال تحقق التهديدات السيبرانية، كما يمكن من إعادة الوضع لما كان عليه في أسرع وقت بما لا يؤدي إلى تعطيل عمليات الانتاج والتشغيل. كما عرفها شحاته (2022) بأنها "مجموعة السياسات والعمليات والأساليب الرقابية المصممة لحماية المعلومات والأنظمة من الهجمات الالكترونية والاختراق الأمني والتي قد تحد من إمكانية تحقيق نظام الأمن السيبراني لأهدافه المرجوة، المتمثلة في إتاحة المعلومات والسرية وسلامة العمليات التشغيلية". كما عرفها Melaku (2023) بأنها عملية اكتشاف التهديدات والثغرات الأمنية للمؤسسة من أجل تحديد سيناريو الهجوم، واتخاذ قرار بشأن كيفية معالجة مخاطر الأمن السيبراني. ومن ثم يكون الهدف الرئيسي لتحليل وتقييم مخاطر الأمن السيبراني هو تحديد التهديدات السيبرانية، وتصنيف الأصول التكنولوجية وفقا لأهميتها، وتحديد نقاط الضعف في النظام، وتنفيذ ضوابط أمنية فعالة للتخفيف من المخاطر المحددة، ويدعم هذا النهج الاستباقي تحديد وتحليل وتقييم ومعالجة الهجمات والمخاطر الأمنية بناءً على التأثير السلبي المحتمل للهجمات الإلكترونية التي قد يتم شنها على المؤسسة (Melaku, 2023).

وترى دراسة عطية (2021) أن مجلس إدارة الشركات هو المسؤول عن إدارة المخاطر السيبرانية وذلك بحسب طبيعة النشاط وحجم تلك الشركات وعملياتها والقطاع الذي تنتمي إليه، وقد تنشئ الشركة إدارة مستقلة لذلك الغرض، كما تتضمن مسؤوليات مجلس الإدارة وضع استراتيجية لتحديد المخاطر والتعامل معها وإدارتها، وكذلك تحديد

[5] نقلاً عن: أبو الخير (2023).

مستويات الخطر المقبول، ووضع الإجراءات التنفيذية للتعامل مع كافة أنواع المخاطر ومن بينها بطبيعة الحال مخاطر الأمن السيبراني.

ويرى Bucsa (2021) أن نظام إدارة مخاطر أمن المعلومات يجب أن يتضمن ثلاث مقومات؛ **السرية** (Confidentiality) بما يضمن فرض المستوى المطلوب من السرية في كل نقطة معالجة للبيانات ويمنع الكشف غير المصرح به؛ **والنزاهة** (Integrity) بما يضمن حماية سلامة البيانات عند توفيرها لضمان دقة المعلومات ومنع التعديل غير المصرح به عليها؛ و**التوفر** (Availability) بما يضمن الاستقرار والوصول في الوقت المناسب إلى البيانات والموارد للأشخاص المرخص لهم. ولتحقيق تلك المقومات يجب أن يتوافر في نظام أمن المعلومات ثلاث مكونات رئيسية وهي؛ **الإجراءات** التي تكفلها سياسات نظام أمن المعلومات؛ و**الأشخاص** سواء مستخدمو أو مسؤلو نظام المعلومات الذين يمكنهم ضمان أمن النظام من خلال اتباع الإجراءات؛ و**المكونات المادية** لنظام أمن المعلومات.

كما ترى دراسة Teimoor (2021) أن هناك نوعين من الأساليب لحماية أنظمة قواعد البيانات من الهجوم السيبراني:

أ- القضاء على المخاطر الأمنية، مثل المصادقة على الدخول للنظام والتي تحد من احتمالية الهجمات السيبرانية.

ب- الاستفادة من استخدام أداة تقنية جديدة لها تأثير كبير على أمان المعلومات مثل جدران الحماية النارية firewall، ومراقبة البيانات في الوقت الفعلي.

وترى دراسة Zbar (2022) أن عملية إدارة المخاطر السيبرانية تشمل على مجموعة من الوظائف وهي:

- **وظيفة تقنية المعلومات:** هي المسئولة عن تكنولوجيا المعلومات ضمن إدارة المخاطر وتقوم بتوفير أجهزة الكمبيوتر وملحقاتها ضمن المواصفات بما يتناسب مع احتياجات المنشأة، وتوفير الأجهزة المساعدة، إضافة إلى صيانة تلك الأجهزة والمعدات.
- **وظيفة تطبيقات تكنولوجيا المعلومات:** وهي مسئولة عن معالجة المعلومات باستخدام أنواع مختلفة من تطبيقات تكنولوجيا المعلومات، والسماح بالوصول إلى المعلومات من خلال تطبيقات تكنولوجيا المعلومات من قبل المستخدمين. إضافة إلى تخزين المعلومات في قاعدة البيانات وأجهزة الكمبيوتر وأجهزة تخزين البيانات المركزية (النسخ الاحتياطية) وأجهزة التخزين المحمولة.
- **وظيفة الشبكة:** وهي المسئولة عن الشبكات المحلية أو الخارجية والوصول الآمن إلى تكنولوجيا المعلومات، وتقوم بمهام تبادل المعلومات، مشاركة البرامج، مشاركة الأجهزة مثل الطابعات والكاميرات، إضافة إلى إنشاء مجموعات عمل حيث تتيح الشبكات إمكانية إنشاء مجموعات عمل وتخصيص جزء من مساحة التخزين على الشبكة لأعضاء هذه المجموعة بعيدا عن بقية الإدارة المركزية للشبكة.

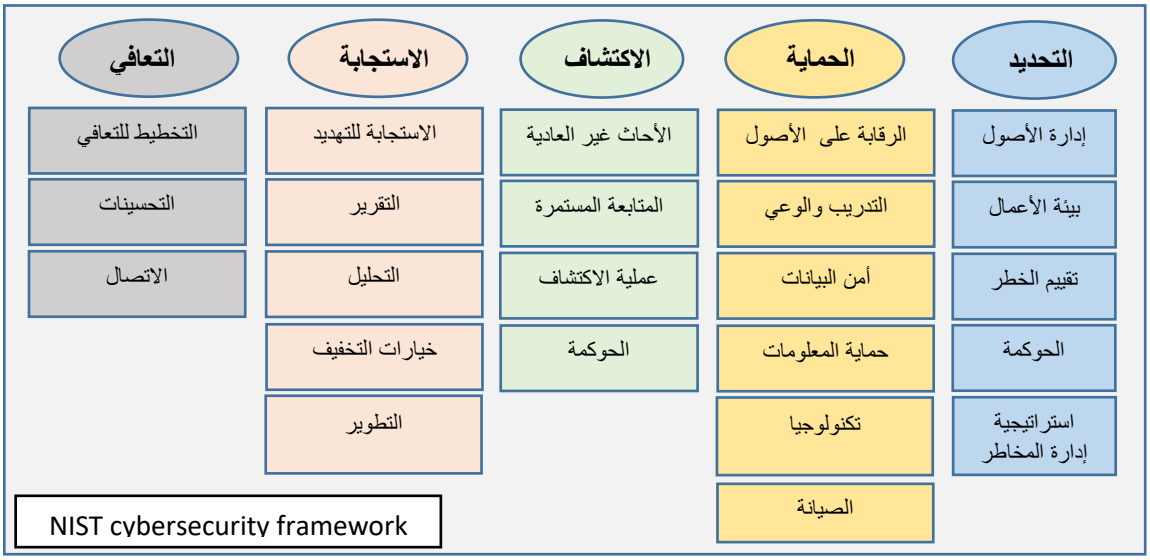
- **وظيفة البنية التحتية:** وهي المسئولة عن تسهيل التفاعل بين مختلف الأطراف المعنية مثل العملاء، الموردين، الشركاء، المقاولين، الجهات الحكومية، ولها مستويات مختلفة من الوصول إلى المعلومات بناءً على دورها الذي سيتم تحديده، و أهم المهام التي تقوم بها توفير الكابلات، والخوادم وتكوين وسائط تخزين البيانات، وتوفير المعدات ومستلزمات البنية التحتية، وإنشاء قاعة اجتماعات افتراضية ومرافق للتدريب والعرض.
- **وظيفة أمن المعلومات:** وهي المسئولة عن الجوانب الأمنية لبيئة إدارة المخاطر السيبرانية، وتتضمن التوعية بأمن المعلومات والتي تتطلب تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية أنظمة وشبكات الحاسب الآلي، وكذلك حماية المعلومات بكافة أشكالها في مراحل الإدخال والمعالجة والنقل والاسترجاع. إضافة إلى إدارة الوصول الآمن، والحماية من البرمجيات الضارة، وإدارة حوادث أمن المعلومات.

كما أشار أبو الخير (2023) إلى أن هناك ثلاث خطوط دفاعية لتحقيق الأمن السيبراني، حيث يتمثل الخط الدفاعي الأول في مديري وحدات الأعمال جنباً إلى جنب مع وظيفة تقنية المعلومات، بينما يمثل الخط الدفاعي الثاني في إدارة مخاطر أمن المعلومات بما توفره من خبرات لتنفيذ ومتابعة فاعلية إجراءات وضوابط الأمن السيبراني، أما الخط الدفاعي الثالث، فهي المراجعة الداخلية.

ونظراً لأهمية إدارة مخاطر الأمن السيبراني فقد وضعت العديد من المنظمات والجهات أطراً تتعلق بإدارة المخاطر السيبرانية، وتتضمن معظم معايير الأمان وأفضل الممارسات، وبصفة عامة تتضمن تلك الأطر ثلاث عمليات رئيسية ومترابطة: **تقييم** المخاطر السيبرانية، **وتخفيف** المخاطر المحددة والمُحَلَلَة، و**التقييم الدوري** لإدارة مخاطر الأمن السيبراني نفسها، غير أن هناك أطراً تضمنت معايير إضافية أكثر تفصيلاً (Melaku, 2023).

ومن أهم تلك الأطر التي تم تطويرها، ما قامت به جمعية رقابة ومراجعة نظم المعلومات Information System Audit and control Association (ISACA) والتي اهتمت بتطوير سلسلة من النماذج والأطر لتمكين إدارة الشركات من حوكمة تكنولوجيا أطلق عليها Control Objectives for Information and related Technologies (COBIT) وانتهت تلك المحاولات التي استمرت لأكثر من 25 عام بتطوير إطار COBIT2019 (فريد، 2022؛ عطية 2021)، بهدف مراقبة عمليات تكنولوجيا المعلومات وحماية أمن المعلومات وربط أهداف تكنولوجيا المعلومات مع أهداف المؤسسة، من خلال توفير إرشادات عامة لجميع العمليات التي يتم فيها عرض أنشطة تكنولوجيا المعلومات بالتفصيل وشرح كيفية تنفيذها (السجيني وآخرون، 2023) . وقد اختبرت دراسة السجيني وآخرون (2023) دور إطار COBIT2019 في إدارة مخاطر عمليات تكنولوجيا المعلومات بالبنوك وتوصلت إلى وجود تأثير معنوي لتطبيق هذا الإطار على تنفيذ الحوكمة السليمة لتكنولوجيا المعلومات، وتحسين إدارة المخاطر السيبرانية بالبنوك.

كما طور المعهد الوطني للمعايير وتكنولوجيا المعلومات National Institute of Standards and Technology (NIST) إطاراً لتحسين البنية التحتية للأمن السيبراني بهدف مساعدة الشركات على تخفيض الآثار المحتملة لمخاطر الأمن السيبراني والذي يتكون من المحاور الأساسية التالية؛ التحديد، والحماية، والاكتشاف، والاستجابة، والتعافي، وتتكون كل مرحلة من مجموعة من الأنشطة المختلفة لإدارة المخاطر السيبرانية كما يتضح من الشكل رقم (1) (Melaku, 2023).



شكل 1: إطار NIST للأمن السيبراني، نقلاً عن: Melaku (2023)

ومن أهم معايير إدارة مخاطر الأمن السيبراني، تلك الصادرة عن منظمة الأيزو[6]، خاصة معيار رقم ISO 27001، الصادر عام 2005، والذي يختص بتحديد القواعد المرتبطة بأمن وحماية تكنولوجيا المعلومات، من حيث كيفية التصميم و التطبيق والرقابة والتطوير المستمر لنظام إدارة تكنولوجيا المعلومات، إضافة إلى التقييم المستمر للمخاطر التكنولوجية التي يتعرض لها النظام. ويقوم المعيار على أربعة مراحل أساسية وهي؛ **التخطيط** لبناء وتشغيل النظام، و**تنفيذ** الخطة الموضوعة وتشغيلها، و**التحقق والتقييم** من خلال المراجعة الدورية للتنفيذ لمطابقة تحقيق الأهداف، واتخاذ الإجراءات اللازمة لصيانة وتحسين النظام، وتحديد النقاط الأساسية التى يجب القيام بها بعد التطبيق لتأمين وحماية الأصول التكنولوجية لتجنب مخاطر التشغيل الإلكترونى. إضافة إلى المعيار ISO 38500، والذي يقوم على مجموعة من القواعد وهي؛ التحديد الواضح والدقيق لمهام ومسئوليات إدارة تكنولوجيا المعلومات، ووضع إستراتيجية كاملة للتخطيط بما يتفق مع أهداف ومتطلبات المؤسسة ، وأن يتم اقتناء تكنولوجيا المعلومات المناسبة وفقاً لأسباب منطقية ومحددة، والتأكد من أن الأداء التكنولوجى يسير وفقاً للخطوات الموضوعة، وتحقيق التوافق بين تكنولوجيا المعلومات والقوانين واللوائح ذات العلاقة بها، ومراعاة الموارد المالية والكفاءات البشرية اللازمة لإدارة وتشغيل النظام.

(6) نقلا عن: الخرينج (2022)

وفي مصر، فقد اهتمت الدولة المصرية ومؤسساتها بالأمن السيبراني وإدارة مخاطره، فقد اهتم الدستور المصري بتلك القضية، حيث نص في مادته رقم 31 على أن "أمن الفضاء المعلوماتي جزء أساسى من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه ، على النحو الذي ينظمه القانون ".

وفي عام 2009 قام الجهاز الوطني لتنظيم الاتصالات بتأسيس المركز المصري للاستجابة لطوارئ الإنترنت والحاسب (المجلس الأعلى للأمن السيبراني) التابع لمجلس الوزراء ويرأسه وزير الاتصالات وتكنولوجيا المعلومات، بحيث يكون مسؤولاً عن الاستجابة لحوادث أمن الكمبيوتر والمعلومات، وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية والتعاون مع الهيئات الحكومية والمالية وأي قطاعات معنية بالبنية التحتية المعلوماتية الحرجة، كما يوفر المركز أيضاً الإنذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية الضخمة ضد البنية التحتية للاتصالات في مصر.

ومنذ عام 2012 يقدم المركز المصري للاستجابة لطوارئ الانترنت والحاسب الدعم لمختلف قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية، من أجل مساعدتهم على مواجهة مخاطر الأمن السيبراني، واتخاذ جميع الإجراءات المرتبطة بتلك المخاطر. ويتكون المركز من أربع إدارات رئيسية وهي؛ مراقبة المخاطر والتعامل مع الحوادث السيبرانية، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الضارة، وفحص الثغرات واختبار الاختراقات، ويقدم المركز أيضاً الانذار المبكر ضد انتشار البرمجيات الضارة والهجمات السيبرانية الضخمة ضد البنية التحتية التكنولوجية في مصر (البغدادي، 2021).

وفي إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبرانى والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، قام المجلس الأعلى للأمن السيبراني بوضع الاستراتيجية الوطنية للأمن السيبراني (2017–2021)، حيث تم وضع هدفاً استراتيجياً يتمثل في "مواجهة المخاطر السيبرانية وتعزيز الثقة في البني التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه". حيث تضمنت تلك الاستراتيجية مجموعة من البرامج تتضمن؛ برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية، برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، برنامج لحماية الهوية الرقمية، برنامج المواطنة الرقمية، وتفعيل البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية، برنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني، برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها.

وقد تم تحديث تلك الاستراتيجة بالاستراتيجية الوطنية للأمن السيبراني (2023–2027) والتي أكدت على أن وجود تلك الاستراتيجة ينبع من ركيزتين أساسيتين، الأولى تتمثل في التصدي للحوادث السيبرانية التي تتزايد بشكل واضح، والثاني هو ضرورة تطوير الكوادر البشرية وتطوير صناعة وطنية تسهم في زيادة الناتج المحلي بما يقدم فرصاً للسوق المصرية. وقد غطت تلك الخطة ستة مجالات من خلال برامج تحققها وتشمل؛ بناء إطار تشريعي متكامل، وتغيير ثقافة المجتمع حول الأمن السيبراني، وتعزيز الشراكة الوطنية، وبناء دفاعات قوية وقادرة على الصمود، وتشجيع البحث العلمي وتعزيز الابتكار والنمو، وتعزيز التعاون الدولي.

كما تم إصدار قانون مكافحة جرائم تقنية المعلومات المعروف بـ"مكافحة جرائم الإنترنت " رقم 175 لسنة 2018 ولائحته التنفيذية، وقانون حماية البيانات الشخصية رقم 151 لسنة 2020. إضافة إلى مسودة قانون الأمن السيبراني (قيد الإعداد).

أضافة إلى أحكام قانون البنك المركزي والجهاز المصرفي الصادر بالقانون رقم 194 لسنة 2020، والتي تطرقت إلى مفهوم البنوك الرقمية وما تقدمه من خدمات مصرفية عبر القنوات أو المنصات الرقمية باستخدام التقنيات التكنولوجية الحديثة.إضافة إلى أحكام القانون رقم 5 لسنة 2022 والخاص بتنظيم وتنمية استخدام التكنولوجيا المالية في الأنشطة المالية غير المصرفية والذي تضمن ضمن قواعد منح الترخيص أن يتوافر لدى الشركة التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين اللازمة لمباشرة النشاط، ونظم لحماية البيانات الخاصة بالمتعاملين من الاختراق الالكتروني والهجمات السيبرانية.

وفي ضوء جهود الهيئة العامة للرقابة المالية لدعم الأمن السيبراني تم البدء بنشاط التأمين، من خلال الكتاب الدوري رقم 3 لسنة 2023 بشأن إجراءات تعزيز الأمن السيبراني بشركات التأمين. ثم تم إصدار قرار الهيئة رقم 139 لسنة 2023 بشأن التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين، وذلك لمزاولة أنشطة الخدمات المالية غير المصرفية، والذي تضمن قواعد تفصيلية بشأن البنية التكنولوجية، وإطار عمل إدارة المخاطر السيبرانية. واستكمالاً لذلك فقد صدر الكتاب الدوري رقم (3) في يوليو 2024 الصادر عن الهيئة العامة للرقابة المالية، والذي ألزم مؤسسات قطاع التمويل غير المصرفي باتخاذ كافة الإجراءات الواجبة لتعزيز منظومة الأمن السيبراني لديها وحماية الأنظمة والبيانات ذات الحساسية، على أن يشمل ذلك كل من التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين الواردة في قرار مجلس إدارة الهيئة رقم 139 لسنة 2023.

3-8 أهمية إدارة الأمن السيبراني في البنوك وغيرها من المؤسسات المالية

حدث تطور هائل في الفترات الأخيرة في اعتماد البنوك على تكنولوجيا المعلومات سواء في تشغيل عملياتها، أو في تنويع خدماتها التي تقدمها للعملاء، إلى أن ظهر ما يعرف بالبنوك الالكترونية E-banks والتي تقدم خدمات مصرفية الكترونية. ويهدف ذلك إلى إمكانية وصول البنك لقاعدة عريضة من العملاء، وسرعة انجاز العمليات،

وتجاوز الحدود الجغرافية، مع إمكانية خفض التكاليف التشغيلية، وزيادة كفاءة العمليات البنكية وتقديم خدمات جديدة. ويتطلب ذلك العديد من الوسائل الالكترونية مثل وسائل الدفع الالكترونية من خلال بطاقات الائتمان، والمحافظ النقدية الالكترونية، والتعامل على الحسابات عن بعد والتي أصبحت متاحة على مدار الساعة إلى غير ذلك من الخدمات البنكية الالكترونية، غير أن الاعتماد الموسع على تكنولوجيا المعلومات والاتصالات في عمليات وخدمات البنوك يصاحبة زيادة في درجة المخاطر السيبرانية التي تواجهها البنوك ويواجهها العملاء المتعاملين على تلك الخدمات، فالبنوك هي هدف رئيسي للمهاجمين بسبب الكميات الهائلة من البيانات الحساسة والمعاملات المالية التي تتضمنها (Hassan et al., 2024; Stanikzai and Saleh, 2021) .

ففي مارس 2024 قدمت شركة ماكينزي[7] (McKinsey, 2024) تقريراً بشأن تبني المؤسسات المالية للتقنيات المستحدثة، من واقع دراسة استقصائية قامت بها الشركة على البنوك والمؤسسات المالية بعنوان "الحرب السيبرانية على الأبواب: مخاطر لتخفيض المخاطر التكنولوجية بالمؤسسات المالية". وتوصلت الدراسة إلى أن هناك اتجاها قوياً نحو ستخدام اربع تقنيات جديدة، وأنه على الرغم من أهمية ما توفره تلك التقنيات من فوائد ومنافع تشغيلية لتلك المؤسسات، إلا أنها تفتح المجال للمزيد من المخاطر السيبرانية والتي تمتد إلى ما هو أبعد من المخاطر القائمة، الأمر الذي يتطلب المزيد من الجهود والانفاق لحماية الأمن السيبراني للمؤسسات المالية وإدارة المخاطر المرتبطة بها.

وقد تأخذ المخاطر السيبرانية التي تتعرض لها البنوك العديد من الأشكال منها استهداف البنية التحتية التكنولوجية للبنك بما يؤثر سلباً على عمليات البنك وتسوياته، واستغلال التغراث في النظام والبرمجيات، واختراق البيانات وسرية الحسابات واحتمالية محو البيانات، واستهداف الهواتف الذكية التي تتصل بالحسابات الشخصية وتستخدم لتنفيذ العمليات البنكية الالكترونية، وقد يكون ذلك بسبب السرقة أو الاحتيال الالكتروني، إضافة إمكانية الوصول إلى البيانات المالية والمعلومات الشخصية للعملاء واستغلالها بطرق غير قانونية (Dawodu et al., 2023; Choo, 2011). وقد يتم ذلك من خلال البرمجيات الفيروسية، والرسائل والروابط المزيفة عبر وسائل الاتصال إلى غير ذلك من الجرائم السيبرانية (البغدادي، 2021).

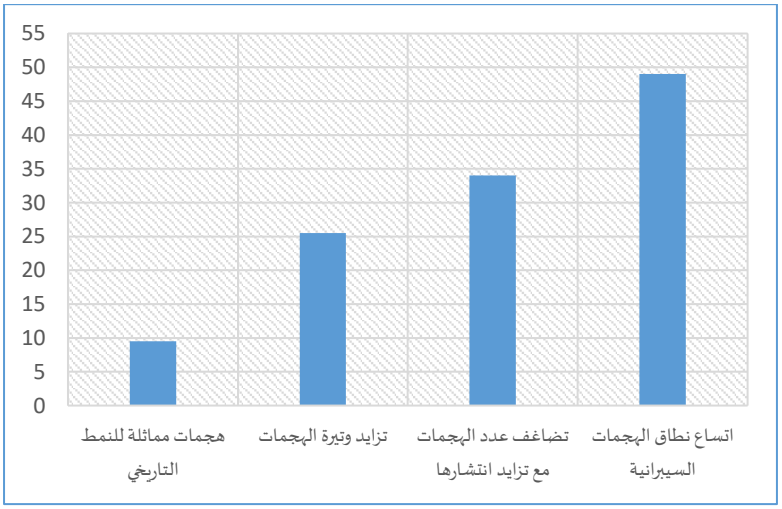
وقد يؤدي ذلك إلى العديد من الأثار السلبية على البنوك والمؤسسات المالية منها؛ فقدان الثقة لدى العملاء والمستثمرين، مما يؤثر سلبا على سمعة الشركة ويؤدي إلى خسائر مالية كبيرة، إضافة إلى احتمال أن تؤدي تلك الهجمات إلى تعطيل خدمات البنوك والمؤسسات المالية، مما يؤثر على العمليات المالية وقد يتسبب في التأثير

[7] شركة McKinsey هي استشارات إدارية عالمية تأسست في 1926، وتعتبر من أكبر 3 شركات استشارات على مستوى العالم. وتقدم خدمات استشارية للشركات في مجموعة واسعة من القطاعات، بما في ذلك الصناعة، الرعاية الصحية، الخدمات المالية، والتكنولوجيا.

على العمليات وكفاءة التشغيل وتوقف الأعمال (Hassan et al., 2024; Dawodu et al., 2023; Al-Alawi and Al-Bassam, 2020).

وبالفعل قد كان القطاع المصرفي هدفًا رئيسيًا للهجمات الإلكترونية بسبب البيانات الهامة التي يحتوي عليها (Firoozi and Mohsni, 2023). فقد أشارت دراسة الاتحاد المصري للتأمين أن قطاعات الأعمال بكافة انواعها معرضة للمخاطر السيبرانية مقدمة ترتيباً بحسب القطاعات الاكثر تعرضاً للجرائم السيبرانية بحسب تكرارية التعرض للخطر وشدته، وجاء أول تلك القطاعات القطاع المصرفي (الاتحاد المصري للتأمين، 2019).

كما أشار تقرير موجز سياسات صندوق النقد العربي (2019)، أن القطاع المصرفي شهد بالعام 2016 هجمات سيبرانية تجاوزت القطاعات الأخرى بنسبة 65% بما يمثل نسبة زيادة 29% عن العام السابق، وفق تقديرات البنك الدولي. وأنه وفقاً للخسائر المحققة في المؤسسات المالية نتيجة الاختراقات السيبرانية على مستوى 50 دولة، فإن متوسط الخسائر المحتملة نتيجة الخطر السيبراني تصل إلى 9% من صافي دخل البنوك على مستوى العالم وهو ما يعادل 100 مليار دولار، وقد تصل تلك النسبة إلى 33% من صافي دخل البنوك وهو ما يعادل من 270–350 مليار دولار إذا ما تضاعفت الهجمات السيبرانية، وهو ما يوضحه الشكل التالي:



شكل 2: تكلفة الخسائر المحتملة للهجمت السيبرانية في قطاع الخدمات المالية كنسبة من صافي الدخل

المصدر: صندوق النقد العربي 2019

وقد دفع ذلك البنوك المركزية العربية إلى تشديد الرقابة والزام البنوك بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية (صندوق النقد العربي، 2019).

كما أشار تقرير لصندوق النقد الدولي (IMF,2024) أن خسائر المخاطر السيبرانية تضاعفت أربعة أضعاف منذ عام 2017، كما أن القطاع المالي على وجه الخصوص كان عرضة للمخاطر السيبرانية، إذ عادة ما يتم استهدافه لسرقة الأموال أو تعطيل الأنشطة الاقتصادية، حيث أورد التقرير أن الهجمات على شركات القطاع المالي بلغت خمس الإجمالي، وكانت البنوك هي الأكثر عرضة لتلك الهجمات. كما أن الحوادث التي يتعرض لها القطاع المالي قد تؤدي إلى تهديد الاستقرار المالي والاقتصادي إذا ما أدت إلى تآكل الثقة في النظام المالي، أو

تعطلت الخدمات الضرورية، أو انتقلت الآثار والتداعيات إلى مؤسسات أخرى، ولا شك أن ذلك يتطلب وضع استراتيجيات وطنية كافية لحماية الأمن السيبراني، مصحوبة بأطر تنظيمية وقدرات رقابية فعالية، بما يضمن تعزيز قوة القطاع المالي. (IMF, 2024)

لذلك، تبذل الشركات –خاصة المؤسسات المالية– جهودًا علاجية لتحسين ضوابط الأمن السيبراني الخاصة بها واتخاذ إجراءات تصحيحية مع العملاء والأطراف المتضررة الأخرى (Jaing et al., 2022)، ويمكن أن يشمل ذلك استخدام أحدث التقنيات للكشف عن الهجمات السيبرانية والدفاع عنها، وتوفير التدريب اللازم للموظفين حول أفضل الممارسات للأمن السيبراني، وتطبيق سياسات صارمة لحماية البيانات. وقد أصدرت بعض المنظمات الدولية مثل صندوق النقد الدولي، وبنك التسويات الدولي، والبنك الدولي أرشادات خاصة تتعلق بإدارة الأمن السيبراني في المؤسسات المالية، إضافة إلى الأطر العامة والارشادات المقدمة من جهات أخرى لإدارة الأمن السيبراني بصفة عامة مثل لجنة الأوراق المالية والبورصات الأمريكية، والمعهد المحاسبين القانونيين الأمريكي (عثمان، 2023).

وقد توصلت دراسة الخرينج وأخرون (2022) إلى أن حوكمة تكنولوجيا المعلومات تسهم في الحد من مخاطر الأمن السيبراني بالبنوك التجارية، من خلال المساهمة الفعالة في تصميم وتحسين إدارة المخاطر السيبرانية. وفي هذا السياق اختبرت دراسة Gatzert and Schubert (2022) دور إدارة مخاطر الأمن السيبراني على قيمة البنوك في السوق الأمريكي، وقد قامت الدراسة على أساس تحليل المحتوى النصي لتحديد وتصنيف البنوك من حيث إدارتها للخطر السيبراني، اعتماداً على ما تقوم ما تفصح عنه في تقاريرها السنوية. وتوصلت الدراسة إلى أن الشركات التي تنتمي إلى قطاع البنوك، والتي تتمتع بدرجة أعلى من الوعي بالمخاطر السيبرانية من المرجح أن تنفذ إدارة المخاطر السيبرانية، كما توصلت الدراسة إلى وجود علاقة إيجابية ومعنوية بين إدارة المخاطر السيبرانية وقيمة الشركة.

ومن هنا تبرز أهمية دراسة أثر مخاطر الأمن السيبراني وإدارته على أحكام المستفيدين ومقدمي التمويل للبنوك لاسيما المستثمرين في الأسهم والعملاء.

8-4 الوضع في مصر فيما يتعلق بإدارة المخاطر السيبرانية في القطاع المصرفي:

اهتم البنك المركزي بحماية الأمن السيبراني في القطاع المصرفي[8] ووضع أهداف الامن السيبراني وحددها في المساعدة على حماية أصول المؤسسات المالية ومواردها من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية، بما يسمح لها بمواصلة مهماتها. وركزت أهداف الأمن السيبراني وفقاً للبنك المركزي المصري على ضمان عدم تضرر المؤسسات المالية، ويتمثل ذلك في تقليل احتمالات سوء الأداء أو ظهور أي تهديد والحد من الأضرار الناجمة عنها، وضمان رجوع العمليات العادية إلى حالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة

(8)https://www.cbe.org.eg/ar/cybersecurity

في أعقاب وقوع حادث أمني. وقد اضطلع البنك المركزي المصري بدوره في توفير التنسيق والقيادة لجهود الأمن السيبراني للقطاع المصرفي والمالي، وتعزيز أنشطة الاستجابة للحوادث السيبرانية والتعافي منها، ومشاركة المعلومات الأمنية وتحليلها، وذلك من خلال إنشاء أول مركز قطاعي في مصر للاستجابة لطوارئ الحاسب الآلي للقطاع المالي، وقد أصدر البنك المركزي المصري **إطار الأمن السيبراني التنظيمي** للمساعدة في الحفاظ على بيئة عمل وبنية تحتية تتمتع بأعلى درجات الأمن والحماية للبيانات والمعلومات. ووفقاً لهذا الإطار، يتألف قطاع الأمن السيبراني من الإدارات الآتية[9]:

- **مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي**، ويختص بالتعامل مع الحوادث السيبرانية وطوارئ الانترنت داخل القطاع المالي والمصرفي، من خلال التنبؤ المبكر بالحوادث الأمنية ومواجهتها والتخفيف من آثارها ومنع تكرار حدوثها، وتحليل الأدلة الرقمية والثغرات الأمنية الخاصة بالجرائم السيبرانية لمعرفة مسبباتها ومنع تكرارها.
- **الإدارة المركزية لجاهزية الأمن السيبراني**، وتختص بتحديد أفضل الممارسات والمعايير الدولية وإدراجها ضمن القواعد والتعليمات الرقابية الصادرة للبنوك، وتحديد مقياس مرجعي مستقل لجاهزية الأمن السيبراني لكل المؤسسات الخاضعة لإشراف البنك المركزي المصري. كما تختص بإجراء تقييمات ذاتية وفنية مستقلة للقطاع المصرفي والمالي حول مدى جاهزيته، كذلك قدرة واستعداد البنوك والمؤسسات المالية لإدارة الأمن السيبراني، والتأكيد على ضمان تطبيق مستويات الوقاية من المخاطر السيبرانية المحتملة بهذه البنوك والمؤسسات المالية، وضمان عملية التحسين المستمر. إضافة إلى العمل على تعزيز القدرات التقنية للعاملين بالقطاع المالي من خلال توفير دورات تدريبية احترافية.
- **الإدارة المركزية لخدمات الأمن السيبراني**، وتختص بتقديم الخدمات والاستشارات التقنية المرتبطة بالأمن السيبراني للمؤسسات المالية والبنوك، ومراجعة واعتماد الأمن السيبراني بالمنظومات التقنية البنكية ومختلف التطبيقات المالية، للتحقق من تطبيق معايير الأمن القياسية قبل إصدار التراخيص اللازمة لطرحها والعمل بها في السوق المصرية. كذلك وضع لائحة بالضوابط والتعليمات الرقابية المرتبطة بآليات وأُطر التأمين والحماية ضد الاختراقات الإلكترونية، ومتابعة تعميم ذلك لضمان توفير متطلبات الأمن والجودة عند تطوير أو شراء التطبيقات التقنية. كما تقوم هذه الإدارة بإجراء الدراسات والبحوث والتطوير في مجال الأمن السيبراني، وتحفيز الابتكار التكنولوجي ونقل أحدث التكنولوجيات المستخدمة في هذا المجال، وتنمية المهارات التقنية لمواكبة التطورات المتسارعة.

(9) https://www.cbe.org.eg/ar/cybersecurity/the-cybersecurity-organizational-structure

- **الإدارة العامة للمشروعات والدعم الاستراتيجي**، وتختص بوضع وإدارة خطط جميع المشاريع على نحو تكاملي للقطاع والتأكد من تخصيص الموارد لها لتحقيق الأهداف، ومتابعة التنفيذ مع إجراء التقييم المستمر لتحسين أداء ونتائج ومخرجات هذه المشاريع؛ وكذلك المساعدة في وضع وتطوير استراتيجية القطاع وتحديد مؤشرات لقياس الأداء في ضوء أهدافه الاستراتيجية، والتأكد من اتساقها وتوافقها مع الاستراتيجية المؤسسية للبنك المركزي المصري.

كما تضمنت أحكام قانون البنك المركزي والجهاز المصرفي الصادر بالقانون رقم 194 لسنة 2020 مجموعة من القواعد الجديدة التي تطرقت إلى مفهوم البنوك الرقمية وما تقدمه من خدمات مصرفية عبر القنوات أو المنصات الرقمية باستخدام التقنيات التكنولوجية الحديثة. وجاء من بين اشتراطات الحصول على الترخيص لتقديم الخدمات المصرفية الرقمية، تقديم دارسة جدوى مفصلة تتضمن تحديد الشرائح المستهدفة والمنتجات الرقمية المخطط إتاحتها، وكذلك خطط تكنولوجيا المعلومات، وخطط واستراتيجيات الأمن السيبرانى. كما تضمن القانون المشار إليه مهام المعهد المصرفي والذي يتبع البنك المركزي، وتكون من ضمن مهامه تنمية المهارات المتعلقة بنظم وخدمات الدفع وتكنولوجيا وأمن المعلومات (مادة 180). وقد خصص القانون الباب الرابع لتنظيم نظم وخدمات الدفع الالكتروني (مواد 184- 200)، والتكنولوجيا المالية[10] (مواد 201- 206).

وقدم باب العقوبات بالقانون بعض العقوبات بالغرامة و/أو الحبس الناتجة عن مخالفة تلك الأحكام، فعلى سبيل المثال، يعاقب بالغرامة والحبس (أو كلامها) ويعاقب بكلاهما في حال العود، كل من خالف أحكام المواد 184 و185، و206[11]، كما يعاقب بغرامة من نصف مليون إلى مليون من خالف أحكام المادة 197[12].

ونتيجة لأهمية المخاطر السيبرانية التي تتعرض لها الشركات بصفة عامة، والبنوك بصفة خاصة، وما تتبناه من استراتيجيات لإدارة تلك المخاطر، فمن المتوقع أن يكون لدى المتعاملين مع ذلك القطاع الحيوي طلباً متزايداً على الإفصاح حول تلك المخاطر السيبرانية، وما إذا كانت البنوك لديها القدرة على إدارة تلك المخاطر والتعامل معها والحد من آثارها إذا ما وقعت.

إن مخاطر الأمن السيبراني لها بعد تقني وينعكس آثاره على النظام المحاسبي. فمحاسبياً يجب على الإدارة حصر هذه المخاطر وتقدير آثارها وإدارتها، والإفصاح عن ذلك، الأمر الذي سيؤثر على وظيفة الاتصال الإعلامي لنظام المحاسبة المالية بالبنوك.

([10]) تم تعريف التكنولوجيا المالية بقانون 14 لسنة 2020 على أنها، نماذج أعمال أو تطبيقات أو منتجات مالية قائمة على استخدام التكنولوجيا.

([11]) تشير المادة 184 إلى أنه لا يجوز مزاولة نشاط يتضمن نظم الدفع الالكتروني دون ترخيص من البنك المركزي، بينما تشير المادة 185 إلى الشروط الواجبة لمنح الترخيص بتقديم الخدمات الرقمية، بينما تتضمن المادة رقم 206 الاشتراطات المرتبطة باصدار عملات مشفرة أو نقود الكترونية أو الاتجار فيها أو الترويج لها أو اصدار منصات لتداولها أو تنفيذ الانشطة المتعلقة بها دون الحصول على ترخيص من البنك المركزي.

([12]) تشير المادة 197 لا يجوز لمن رخص له تشغيل نظم الدفع الالكتروني القيام بأي إجراء يترتب عليه ايقاف أو انهاء أو التأثير على نشاطه دون الحصول على ترخيص من البنك المركزي.

9- الإفصاح عن إدارة الخطر السيبراني من منظور المحاسبة المالية:

على الرغم من الاتجاه المتصاعد من الشركات للإفصاح عن حوادث الاختراقات التي تعرضت لها، إلا أنه مازال هناك القليل من الإفصاح عن جهود الشركات في إدارة تلك المخاطر السيبرانية وكيفية التعامل معها، الأمر الذي دعا كل من المستثمرون والجهات المنظمة إلى المناداه بتطوير عملية الإفصاح عن إدارة مخاطر الأمن السيبراني، والذي أدى إلى قيام AICPA بتطوير إطاراً للإفصاح والتقرير عن إدارة مخاطر الأمن السيبراني (Frank et al., 2019).

إن الهدف من الإفصاح عن مخاطر الأمن السيبراني وكيفية إدارة تلك المخاطر يتمثل في تزويد المستثمرين والأطراف المعنية الأخرى بمعلومات كافية لتقييم مدى تأثر الشركة بمخاطر الأمن السيبراني. لذا اهتمت العديد من الجهات المنظمة بالافصاح عن المخاطر السيبراينة من خلال ثلاث مستويات؛ المستوى الأول هو الإفصاح عن حالات الهجمات السيبرانية التي تعرضت لها الشركات بالفعل وما ترتب عليه من أثار. والثاني هو الإفصاح عن المخاطر السيبرانية المتوقعة التي قد تتعرض لها الشركات، والثالث هو جهود الشركات في إدارة تلك المخاطر السيبرانية.

وفي هذا الصدد فقد صدر عن لجنة الأوراق المالية والبورصات الأمريكية (SEC) عام 2011 إرشادات تطلب من الشركات الإفصاح عن مخاطر الأمن السيبراني والهجمات السيبرانية إذا كانت تلك المخاطر والهجمات تشكل أخطاراً مادية لأعمال الشركة. ونظراً لتكرار وحجم وتكلفة حوادث الأمن السيبراني، فإن SEC عام 2018 قدمت دليلاً بشأن الإفصاح بمستوياته الثلاثة عن مخاطر الأمن السيبراني يعد امتداداً للدليل السابق عام 2011، أشارت فيه إلى أنه من الضروري أن تتخذ الشركات المقيدة جميع الإجراءات لتقديم إفصاح للمستثمرين عن المخاطر والحوادث المادية المتعلقة بالأمن السيبراني في الوقت المناسب، سواء تلك التي حدثت بالفعل أو المتوقع حدوثها بما في ذلك تلك الشركات التي من المحتمل أن تكون عرضة لمخاطر أمنية سيبرانية جوهرية وإن لم تكن تعرضت بعد لهجوم سيبراني، دون أن يكون هناك الزام بمصطلحات أو محتوى محدد، أو الكشف عن معلومات تفصيلية يمكن أن يعرض جهود الشركة في مجال الأمن السيبراني للخطر، مقدمةً إرشاداً للشركات عند **تقييم العوامل المحددة للإفصاحات** يتمثل في؛ (1) مدى وقوع حوادث سيبرانية سابقة متضمنةً خطورتها وتكرارها، (2) احتمالات الحدوث وأهمية الحدث المحتمل حدوثه، (3) مدى كفاءة الإجراءات المتخذة للحد من المخاطر السيبرانية، (4) تكاليف نظم الحد من مخاطر الأمن السيبراني، بما في ذلك تكلفة التأمين ضد تلك المخاطر، (5) طبيعة عمليات الشركة والتي ترتبط بها مخاطر سيبرانية متلازمة والتكاليف المرتبطة بها واحتمالات حدوث الخطر السيبراني، (6) احتمالية التأثير السلبي والإضرار بالسمعة، (7) القوانين والنظم القائمة التي تخضع لها الشركة فيما يتعلق بالأمن السيبراني، (8) احتمالات التقاضي والعقوبات التنظيمية وتكاليف العلاج المرتبطة بالحوادث السيبرانية (SEC, 2018).

ووفقاً للإصدار 2018، فإن **الافصاح يتضمن** كل من عوامل الخطر السيبراني، وتأثير ذلك الخطر على منتجات الشركات وخدماتها والعلاقات مع العملاء والموردين، وأي إجراءات قانونية متعلقة بالمخاطر السيبرانية، إضافة إلى الإفصاح ضمن القوائم المالية عن الآثار المالية لمخاطر الأمن السيبراني سواء تلك المتعلقة بتكاليف المنع وإدارة مخاطر الأمن السيبراني، أو تكاليف المعالجة أو الأثر المالي والنقدي الناتج عن تلك المخاطر، والأثر على كفاءة العمليات وتقديم الخدمات، إضافة إلى الإفصاح عن كفاءة ودور مجلس الإدارة في مراقبة مخاطر الأمن السيبراني كأحد مسؤولياته في إدارة مخاطر الشركة. كما حدد الإصدار ضرورة أن تقوم الشركة بتحديد ضوابط وإجراءات الإفصاحات والتي تضمن أن يتمكن النظام في الشركة من الإفصاح عن مخاطر الأمن السيبراني بما يتوافق مع المتطلبات التنظيمية للإفصاح، وبما يضمن عدم استغلال الداخليين لتلك الأحداث للتعامل على أسهم الشركة، وعدم الإفصاح الانتقائي (غير العام) لمعلومات جوهرية تتعلق بالأمن السيبراني لأطراف معينة دون النشر العام (SEC, 2018) [13].

وفي 2022 أصدرت SEC تعديلاً بشأن متطلبات الإفصاح المتعلقة بإدارة مخاطر الأمن السيبراني من خلال الإفصاح عن مخاطر الأمن السيبراني غير الهامة الفردية والتي تشكل في مجملها أحداثاً هامة، وإعداد تقرير سنوي حول خبرة مجلس الإدارة في مجال الأمن السيبراني، والسياسات المتبعة لمواجهة مخاطر الأمن السيبراني وكيفية التعامل معها بعد حدوثها مباشرة، والإفصاح الدوري عن سياسات إدارة وحوكمة مخاطر الأمن السيبراني، وتحديد المسؤول عن حوكمة الأمن السيبراني (شرف 2023).

وقدمت دراسة Janvrin and wang (2022) نموذجاً يعكس علاقة الأمن السيبراني بالمعلومات المحاسبية (إطار الحدث، الأثر، والاستجابة) اعتماداً على كل من إطار عمل المخاطر المؤسسية الصادرة عن منظمة (COSO 2017)، وإطار الاتصالات المالية للشركة واستجابة المستثمرين (Blankespoor 2018). ويشير ذلك النموذج إلى أن استجابة الإدارة للمخاطر السيبرانية تأخذ عدة اتجاهات منها الإفصاح عن الأمن السيبراني، إضافة إلى إدارة الأمن السيبراني، بينما استجابة المستثمرين تكون من خلال تعديل أحكامهم بشأن قرارات الاستثمار، ورفع قضايا.

ونظراً لأهمية الإفصاح عن مخاطر الأمن السيبراني وإدارته، ونظراً لعدم التماثل الواضح في تلك المعلومات، فإن أصحاب المصالح يطالبون بالمزيد عن المعلومات حول كل من مخاطر الأمن السيبراني، والانتهاكات التي حدثت، وأيضاً سياسات الشركة لإدارة تلك المخاطر والتعامل مع ما تم من انتهاكات لتحييد أثارها أو الحد منها واستعادة الوضع بأسرع ما يمكن، غير أن ما يتوافر لأصحاب المصالح حول تلك المعلومات هو قدر ضئيل لا يلبي احتياجاتهم الأساسية من تلك المعلومات (Cheong et al., 2021)، إذ يرى شرف (2023) أن ذلك الإفصاح

([13]) هذا الاصدار تضمن قضيتين اضافيتين لم يتم التطرق لهما في الاصدار 2011، الأول يتضمن أهمية سياسات إدارة الأمن السيبراني والافصاح عنها، والثاني يتضمن حظر التداول الداخلي في سياق الأمن السيبراني.

غير نمطي ويتسم بقدر عالي من المرونة ويمنح الشركات الحكم والتقدير في تحديد طبيعة ومحتوى ومدى الإفصاح، وكيفيته، حيث قد تستجيب بعض الشركات للجهود الرامية لزيادة مستوى ذلك الإفصاح، إلا أن الشركات الأخرى قد لا تستجيب لذلك. وهو ما أكدت عليه دراسة Jiang et al. (2022) والتي ترى أن هناك شركات لا تقدم إفصاحات تتعلق بمخاطر الأمن السيبراني بعد حدوث هجمات واختراقات سيبرانية، أو تغير من سلوك إفصاحها عن المخاطر السيبرانية، على الرغم من مطالبة الشركات من قبل هيئة البورصة الأمريكية بضرورة الإفصاح الفوري عن أي اختراقات سيبرانية تعرضت لها الشركة ضمن ملف 10-k. وهو ما يتوافق مع مخرجات المنتدى الاقتصادي العالمي (2022)، والتي ترى بأنه لا يوجد الزام للشركات سوى الكشف عن قدر ضئيل من المعلومات حول جهود إدارة مخاطر الأمن السيبراني وذلك على الرغم من أهمية مخاطر الأمن السيبراني وأنها هي أكثر مخاطر الاستدامة المباشرة والمادية التي تواجهها المؤسسات، والتي تعرض الشركات لخسائر مالية كبيرة وخسارة في السمعة (Frank et al., 2023).

أما في مصر فلم تصدر الهيئة العامة للرقابة المالية متطلبات خاصة للإفصاح عن مخاطر الأمن السيبراني، أو حوادث التعرض لهجمات سيبرانية، أو للإفصاح عن آليات إدرة الخطر السيبراني (يوسف، 2022؛ فريد، 2022)، على الرغم من أن إدارة الخطر هو أحد متطلبات الإفصاح المطلوبة من البنوك من خلال قانون 194 لسنة 2020، إلا أن ذلك الإفصاح ومن خلال مسحاً أجراه الباحث تركزت في الإيضاحات المتممة للقوائم المالية حول الإفصاح عن مخاطر الائتمان، ومخاطر السيولة، ومخاطر السوق والتي قد تتضمن مخاطر سعر الصرف ومخاطر سعر العائد. وبمراجعة نماذج الإفصاح بالبورصة المصرية، اتضح للباحث أن نموذج تقرير الحوكمة **الارشادي** الصادر عن الهيئة العامة للرقابة المالية قد تضمن نصاً يفيد بأن تقوم الشركة بتحديد دور مجلس الإدارة في وضع الإجراءات الوقائية والأدوات والآليات التي تعمل على تأمين تدفق المعلومات والسيطرة على دقة وسلامة البيانات داخل الشركة وحمايتها من التلاعب والاختراق سواء من داخل الشركة أو من خارجها مثل تأمين استخدام الانترنت وأجهزة المحمول ضد الاختراقات والقرصنة.

وقد حاولت بعض الدراسات استكشاف **العوامل والمحددات التي تقف خلف سلوك الشركات للإفصاح** عن مخاطر الأمن السيبراني، حيث ترى دراسة Amir et al. (2018) أن الشركات لا تميل إلى الإفصاح عن الهجمات السيبرانية التي تعرضت لها إلا إذا كان من المحتمل اكتشاف تلك الهجمات من قبل المتعاملين مع الشركة. بينما رأى آخرون أن هناك عوامل أخرى يمكن أن تؤثر في إفصاح الشركات عن مخاطر الأمن السيبراني مثل حجم الشركة وربحيتها وطبيعة الصناعة واعتمادها على تكتولوجيا المعلومات والاتصالات في أنشطتها، واحتمال التأثير السلبي على سمعة الشركة وتعرضها للعقوبات ومدى جوهرية الاختراقات التي تعرضت لها الشركة (شرف، 2023؛ Gao et al. 2020).

وقد اختبرت دراسة D'Arcy and Basoglu (2022) الدوافع التي تقف وراء الإفصاح عن الأمن السيبراني، حيث أشارت الدراسة إلى تركيز الأبحاث السابقة حول العوامل التنظيمية باعتبارها القوى الدافعة لذلك الإفصاح. غير أن الدراسة ركزت على بديلين من الضغط كدوافع لإفصاحات الأمن السيبراني وهما (1) الضغط العام بعد خرق بيانات الشركة و(2) الضغط الناشئ من انتهاكات الشركات المناظرة في الصناعة. وتوصلت الدراسة إلى أن ممارسات الكشف عن الأمن السيبراني للشركات تتأثر بالضغط العام بعد اختراق البيانات وأن هذا الضغط يكون أكثر حدة بالنسبة للانتهاكات الخارجية مقارنة بالانتهاكات الداخلية. غير أن الانتهاكات التي ترتكبها الشركات المناظرة في الصناعة، تؤدي إلى عدد أقل من الإفصاحات المتعلقة بالأمن السيبراني.

كما توصلت دراسة Jiang et al. (2022) إلى أن كل من تكرار الاختراقات السيبرانية للشركة، ورد فعل السوق لتلك الاختراقات والافصاح عنها يؤثر في سلوك الإفصاح عن المخاطر السيبرانية لتلك الشركات، حيث أيدت النتائج أن ردود أفعال السوق السلبية تدفع الشركات إلى الكشف عن تفاصيل إضافية للتخفيف من ردود الفعل السلبية، بما يدعم من فرضيات الاختيار المعاكس المرتبط بعدم تماثل المعلومات، كما توصلت الدراسة إلى أن الشركات التي تعمل في مجال الصناعات ذات المخاطر الأمنية السيبرانية العالية، تقدم المزيد من الإفصاحات مقارنة بالشركات في الصناعات الأخرى.

وفي مجال **شكل وطبيعة الإفصاح** وبتحليل ما تبنته الدراسات السابقة في مجال الإفصاح عن مخاطر الأمن السيبراني، أمكن للباحث استخلاص ثلاث مستويات للإفصاح عن الأمن السيبراني، الأول يتمثل في الإفصاح عن الاختراقات التي حدثت بالفعل وآثارها على قرارات المتعاملين مع الشركة، والثاني يتمثل في الإفصاح عن المخاطر التي يمكن أن تواجهها الشركات والمتمثلة في عوامل الخطر والتي يمكن أن تختلف باختلاف طبيعة عمليات الشركة والقطاع التي تعمل به ومدى اعتماد عملياتها على تكتولوجيا المعلومات والاتصالات والشبكات الدولية، وقد قدمت بعض الدراسات السابقة نتائج تشير إلى تأثير المستوى الأول من الإفصاح وما يترتب عليه من أثار سلبية يتأثر بإفصاح المستوى الثاني. أما المستوى **الثالث** من الإفصاح فيشير إلى الإفصاح عن إدارة المخاطر الاسيبرانية وما تتخذه الشركة من إجراءات للرقابة على تلك المخاطر والسيطرة عليها والحد من آثارها إذا تمت عملية الاختراقات، وهو ما يؤثر على الآثار التفاعلية للمستويين السابقين.

ففي مجال المستوى الأول، توصلت دراسة الرشيدي، وناصر (2019) إلى أن الإفصاح عن التعرض لهجمات سيبرانية (مستوى الإفصاح الأول) أدى إلى انخفاض أسعار الأسهم، وانخفاض حجم التداول بالشركات الأمريكية. كما أوضحت الدراسة وجود فروق معنوية بين طبيعة الإفصاح عن مخاطر الأمن السيبراني في الشركات المصرية في قطاع تكنولوجيا المعلومات والشركات الأمريكية، وأوصت الدراسة بضرورة تقديم هيئة العامة للرقابة المالية تعليماتها للشركات بالإفصاح عن مخاطر الأمن السيبراني. كما أيدت دراسة Tosun (2021) وجود تأثيراً سلبياً

للكشف عن حدوث اختراقات سيبرانية على أسعار أسهم الشركات في الأجل القصير، ويختلف طبيعة ذلك التأثير بطبيعة الاختراق والمعلومات المسربة عن الشركة. كذلك أشارت دراسة Goel and Shawky (2023) إلى أن الشركات غالبًا ما تتردد في الكشف عن معلومات حول الخروقات الأمنية خوفًا من تقديم المعلومات إلى المتسللين، والأمر الأكثر أهمية هو الانخفاض المحتمل في القيمة السوقية للشركة بعد الكشف عن خرق أمني. واستهدفت الدراسة اختبار أثر الاعلان عن الخروقات الأمنية على قيمة الشركة، وتوصلت إلى نتائج تشير إلى أن الشركات تفقد ما يعادل 1% من قيمتها السوقية خلال الأيام التي تحيط بحدث الاختراق الأمني، وذلك بخلاف الآثار الأخرى مثل التأثير على سمعة الشركة، واحتمالية مقاضاة الشركة وما يتبعه من تعويضات قضائية.

وفي مجال المستوى الثاني، فإن الافصاح عن مخاطر الأمن السيبراني المحتملة قد يقدم إشارات للمستثمرين في الأسهم لاتخاذ القرارات الاستثمارية نتيجة تأثيرها على تقييم مخاطر الأسهم. فوفقاً لدراسة Jaing et al. (2022) فإن نظرية أصحاب المصلحة تتنبأ بأن الكشف عن مخاطر الأمن السيبراني يفيد أصحاب المصلحة، فالتقدم التكنولوجي السريع أدى إلى زيادة كمية المعلومات وتوقيتها، مما يضغط على الشركات لتكون أكثر شفافية تجاه أصحاب المصلحة، بما يحد من تكاليف التعاقد والتي تشمل الدعاوى القضائية التي يرفعها أصحاب المصلحة نتيجة لانتهاك الأمن السيبراني، ويحد من عدم التأكد الذي يمكن أن يؤدي إلى خسارة العملاء. لذلك، يشير الإفصاح الاختياري عن مخاطر الأمن السيبراني إلى الثقة المتبادلة والتعاون بين الشركة وأصحاب المصلحة من خلال توفير المعلومات ذات الصلة والتي تساعد أصحاب المصلحة في تقييم الخسائر الحالية والمستقبلية الناجمة عن حدوث الاختراق وما إذا كانوا سيواصلون علاقتهم مع الشركة. وتشير نظرية أصحاب المصلحة بدورها إلى أن الشركات تنظر إلى فوائد الإفصاح عن الأمن السيبراني على أنها أكبر من التكاليف (Jaing et al., 2022). وأكدت دراسة Chen et al. (2023) على ذلك حيث قدمت دليلاً على أن الإفصاح عن عوامل الخطر له محتوى معلوماتي.

وفيما يتعلق بالأثر التفاعلي للمستويين السابقين، فقد توصلت دراسة Kelton and Pennington (2020) إلى أن حدوث الاختراقات السيبرانية له أثر سلبي على الشركات المخترقة، وينعكس إيجابياً على الشركات المنافسة غير المخترقة، وأن الإفصاح المسبق عن مخاطر الأمن السيبراني المحتمل قبل حدوث الاختراقات يحد من تلك الأثار. كما اتفقت دراسة Cheong et al. (2021) مع دراسة Walton et al. (2021) في أن الإفصاح عن مخاطر الأمن السيبراني يحد من عدم تماثل المعلومات، ومن ثم يمكن من التنبؤ بالاختراقات المحتملة، وبالتالي فإن الإفصاح المسبق عن المخاطر المحتملة المرتبطة بالأمن السيبراني يحد من الأثار السلبية للحدوث اللاحق للاختراقات على سمعة الشركة وتكاليف التقاضي، غير أن الإفصاح عن المخاطر المحتملة للأمن السيبراني قد يكون له انعكاس أخر وهو افشاء بعض الاسرار التي قد يستغلها المهاجمون لإحداث اختراقات سيبرانية لاحقة. كما ترى دراسة Kelton (2021) أن الإفصاح المسبق عن المخاطر السيبرانية المحتملة يكون مدفوعاً بتحقيق مصالح

المديرين من خلال تجنب الآثار السلبية على السمعة نتيجة اختراق البيانات. وهو ما أكدته دراسة Chen et al. (2023) والتي وجدت أن الشركات التي تعاني من اختراق البيانات تزيد من حجم الإفصاح عن عوامل المخاطر السيبرانية السيبراني مقارنة بالشركات المناظرة التي لم تتعرض للاختراقات، وأن زيادة عمليات الإفصاح عن عوامل الخطر السيبراني ترتبط طردياً مع درجة خطورة تلك الانتهاكات. أما فيما يتعلق برد فعل السوق تجاه التغير في محتوى الإفصاحات للشركات، فقد وجدت دراسة Chen et al. (2023) أنه على الرغم من عدم وجود رد فعل كبير في السوق إذا تضمنت التقارير السنوية اللاحقة للشركات المخترقة زيادة في الإفصاح عن عوامل خطر الأمن السيبراني، إلا أنه يحدث رد فعل سلبي كبير في السوق إذا خفضت الشركات المخترقة الإفصاحات عن عوامل خطر الأمن السيبراني، بغض النظر عن خطورة الاختراق، مما يعني أن السوق يتوقع زيادة الإفصاحات بعد خروقات البيانات.

أما في مجال المستوى الثالث من الإفصاح، والمتعلق بالإفصاح عن إدارة مخاطر الأمن السيبراني، فترى دراسة Klemash et al. (2020) أن الإفصاح عن إدارة مخاطر الأمن السيبراني يمكن أن يبني الثقة لدى المستفيدين من خلال العرض الشفاف والتأكيد حول كيفية قيام مجلس الإدارة بالقيام بمسؤولياته لإدارة مخاطر الأمن السيبراني والرقابة عليه. وتشير الدراسات السابقة أن المستثمرين غير المحترفين قد يجدون أن الاستثمار في شركة ما يكون أكثر جاذبية عندما تقوم الشركة بالإفصاح الاختياري عن معلومات حول جهود إدارة مخاطر الأمن السيبراني وتؤكد أن هذه الجهود فعالة، ومع ذلك، تجد الدراسات التجريبية أن مدى تأثير الإفصاح الطوعي عن المخاطر على جاذبية الاستثمار يعتمد على ما إذا كان المستثمرون، يعتقدون أن المعلومات التي تم الكشف عنها موثوقة ويمكن الاعتماد عليها Reliable (Frank et al., 2019).

وبالتالي يمكن أن تلعب إدارة مخاطر الأمن السيبراني دوراً حاسماً في تشكيل ثقة المستثمرين وعمليات صنع القرار في سوق الأوراق المالية، وأنه من خلال تنفيذ تدابير قوية للأمن السيبراني يمكن للشركات التخفيف من المخاطر المحتملة وبالتالي تعزيز جاذبيتها للمستثمرين الذين يدركون بشكل متزايد أهمية الأمن السيبراني. فقد أشارت دراسة Frank et al. (2019) إلى أن المستثمرون يهتمون بصورة كبيرة بالهجمات السيبرانية التي تعرضت لها الشركات وذلك عند اتخاذهم القررات الاستثمارية، نتيجة لتأثيراتها السلبية على قيمة الشركة، غير أن الجهود التي تبذلها الشركات لتدنية تلك المخاطر وأثارها والتعامل معها لا تكون دائماً ملحوظة من قبل المستثمرين، خاصة غير المحترفين، مما يخلق نوعاً من عدم التماثل الكبير في المعلومات لهؤلاء المستثمرين عن تلك الجهود من حيث طبيعتها وفاعليتها، بما قد يجعل تلك الاستثمارات أقل جاذبية من حقيقتها، وهو ما تؤيده افتراضات عدم تماثل المعلومات. وبالتالي فإن الإدارة يمكنها جعل الاستثمار في الشركة أكثر جاذبية من خلال تقديم المزيد من الإفصاح عن إدارة المخاطر.

كما توصلت دراسة Yang et al., (2020) إلى أن هناك أثار ايجابية للإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام المستثمرين غير المحترفين، وأن تلك الأثار الإيجابية تتأثر بكل من جودة المعلومات المقدمة والوعي بمخاطر الأمن السيبراني ونية الاستثمار.

كما اختبرات دراسة علي وعلي (2022) أثر الإفصاح عن تقرير إدارة المخاطر السيبرانية على قرارات الاستثمار من خلال دراسة تجريبية على عدد من المحللين الماليين في مصر، حيث يضفي هذا التقرير الثقة في أعمال الشركة في مجال الأمن السيبراني ويخفض من عدم التأكد بشأن احتمالات تعرض الشركة لمخاطر الأمن السيبراني مما يساعد في ترشيد القرارات وتحسين جودة أحكام المستثمرين. وتوصلت الدراسة إلى أن تقرير إدارة المخاطر السيبرانية يقدم معلومات لها تأثير معنوي إيجابي على قرارات الاستثمار في الأسهم، كما أن خصائص المستثمرن (مثل الخبرة ومستوى التأهيل) لها أثر معدل معنوي على تلك العلاقة.

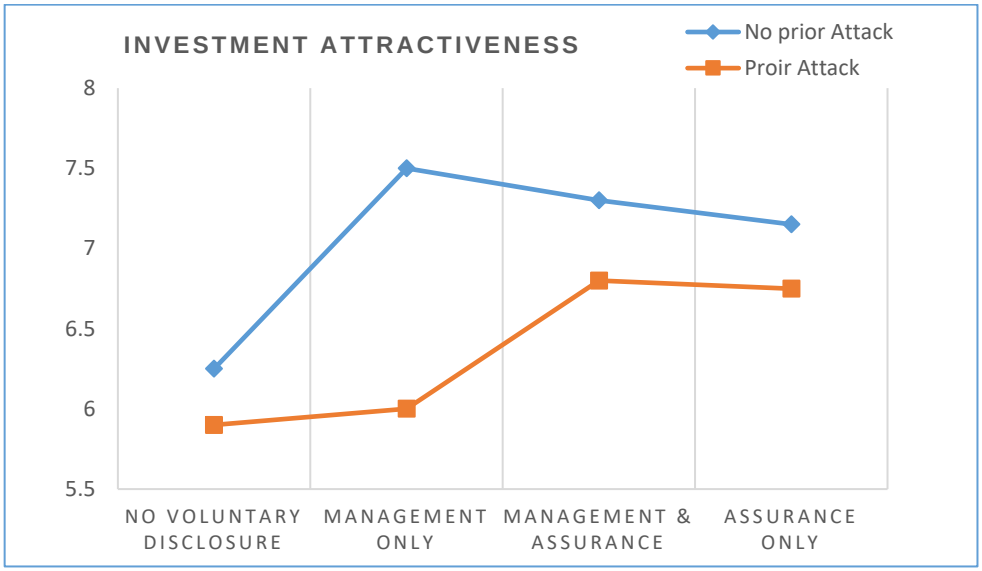
وتوصلت دراسة يوسف (2022) إلى أن مديري إدارة المخاطر بالشركات المصرية يرون أن الإفصاح عن مخاطر الأمن السيبراني قد يضر بمصلحة الشركات واستثماراتها، وذلك على الرغم من أنه يفيد المستثمرين في قرارات الاستثمار، وأن عدم الإفصاح عن الأمن السيبراني يؤدي إلى اتخاذ قرارات استثمارية غير صحيحة. ومن هنا يبرز التعارض في المصالح بين إدارات الشركات ورغبتهم في عدم الكشف عن تلك المعلومات، وبين المستثمرين وما يحتاجونه من معلومات شفافة عن تلك المخاطر.

وبالتالي فإن إفصاح الشركات عن جهود إدارة الأمن السيبراني للأطراف المتعاملين يسهم في الحد من الفجوة المعلوماتية بين ما تقوم به الشركات من إجراءات وما يدركه أصحاب المصالح من تلك الجهود. ومن هنا يأتي أهمية الدور الملزم الذي يجب أن تلعبه الجهات المنظمة للالزام الشركات للافصاح عن تلك المعلومات وبالشكل الذي يضمن حماية أمن الشركات وعدم تعرضها للمخاطر جراء الكشف عن معلومات هامة وسرية قد يستغلها المهاجمون لتحقيق اختراقات أمنية سيبرانية في المستقبل.

كما اختبرت دراسة شرف (2023) تجريبياً أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على قرارات المستثمرين غير المحترفين بمصر وتوصلت الدراسة إلى دليل على أن الإفصاح عن إدارة مخاطر الأمن السيبراني له تأثير معنوي إيجابي على قرارات المستثمرين غير المحترفين بمصر للاستثمار في الأسهم، وتقديراتهم لأسعار الأسهم، وذلك للشركات التي قدمت تقارير عن إدارة مخاطر الأمن السيبراني مقارنة بالشركات التي لم تقدم تلك التقارير، وأن خصائص المشاركين مثل العمر والجنس ومستوى التأهيل المهني لها تأثير معدل معنوي على تلك العلاقة.

وفي سياق المتعلق بالعوامل المؤثرة على علاقة الإفصاح عن إدارة الخطر السيبراني بقرارات الاستثمار فقد أشارت دراسة Frank et al., (2019) إلى أن الإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني تعزز من جاذبية الاستثمار، ويتوقف ذلك على عدد من العوامل منها الكشف عن هجوم الكتروني سابق، وما إذا كان التقرير

عن إدارة مخاطر الأمن السيبراني تم التوكيد عليه من قبل مراجعة مستقل. وقد توصلت الدراسة إلى أن إصدار تقارير الأمن السيبراني وفقاً لمقترح AICPA مع غياب خدمة التوكيد يكون أكثر فعالية عندما لا تكشف الشركة عن هجوم إلكتروني سابق، حيث يكون المستثمرون أقل عرضة للتشكيك في موثوقية التقارير المقدمة. ومع ذلك، فإن الحصول على تأكيد من طرف ثالث لتقرير الإدارة يوفر فائدة أكبر للشركات التي كشفت عن هجوم إلكتروني سابق. وقد لخصت دراسة Frank et al. (2023) تلك النتائج في الشكل التالي:



شكل 3: علاقة الاستثمار بالإفصاح عن إدارة الأمن السيبراني في ظل متغيري خدمات التوكيد، والتعرض لهجوم سابق

المصدر: دراسة Frank et al. (2023)

وبناء على تلك النتيجة يقوم الباحث بتطوير الدراسة التجريبية لتختبر بدائل الإفصاح **مع تحييد خدمة التوكيد، ومع عدم الإفصاح عن اختراقات سابقة**، وبالتالي فمن المتوقع أن الإفصاح سيقدم معلومات تجعل الاستثمار أكثر جذباً للمستثمرين، لكن يبقى الإجابة على تساؤل حول طبيعة بديل الإفصاح ومحتواه وهو ما يحاول البحث الحالي استكشافه، خاصة وأن بعض الدراسات ايدت أن عرض ذات المعلومات بطرق مختلفة يكون له تأثير مختلف على متخذ القرار (Kelton et al., 2010; Hishleifer and Teoh, 2003).

10- تطوير فروض الدراسة:

10-1 تحليل أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرين في أسهمها: وتطوير فرض الدراسة الأول.

إن مخاطر أمن المعلومات يمكن أن يكون لها تأثير طويل الأجل على الأداء التنافسي لأسهم الشركات التي تعرضت لتلك المخاطر، فقد توصلت دراسة (Ali et al. 2022) إلى أن درجة مخاطر الاستثمار في الأسهم أعلى بنسبة 7% للشركات التي تعرضت لانتهاكات أمن المعلومات مقارنة بالشركات المقابلة. كما أن الارتفاع في

مخاطر الاستثمار في الأسهم يكون أعلى إذا كان الاختراق ينطوي على تعريض معلومات سرية للخطر ويكون انتهاكا متكرراً لنفس الشركة. وقد يؤدي ذلك إلى عدم اتخاذ قرارات الاستثمار في أسهم تلك الشركات، وتقييم أسهمها بأنها أسهم ذات مخاطر عالية.

فلا شك أن مجال مخاطر الأمن السيبراني وإدارته يعد من المجالات التي تتضح فيها مشكلة عدم تماثل المعلومات بين إدارة الشركة وأصحاب المصالح، من خلال **مشكلة الخطر الأخلاقي**، والتي تشير إلى أن الإدارة قد تتصرف بطريقة تتعارض مع مصالح أصحاب المصالح الآخرين بحيث لن يتمكن أصحاب المصالح من دحض ادعاء إدارة الشركة بأن ذلك قد حدث بسبب خطأ خارجي عشوائي. وقد تكون أحد تلك التصرفات غير المرغوبة عدم إعطاء الاهتمام الكافي من قبل المديرين لممارسات إدارة الأمن السيبراني والانفاق الكافي لهذا المجال، وهنا يبرز أهمية الإفصاح عن تلك السياسات بما يحد من مشكلة عدم تماثل المعلومات وبالتالي الحد من مشاكل الخطر الأخلاقي (Cortez and Dekker, 2022).

وعلى الجانب الآخر، يمكن الادعاء أنه **وفقاً للاختيار المعاكس** الناتج عن عدم تماثل المعلومات فإن عدم الإفصاح عن مخاطر الأمن السيبراني –خاصة للشركات التي تتميز بارتفاع تلك المخاطر المتزامنة لعملياتها مثل البنوك– فإن المتعاملون يقدرون تلك المخاطر بمستوى مرتفع مقارنة بالبنوك التي تفصح عن طبيعة تلك الأنشطة وكيفية إدارتها. وبالتالي فمن المتوقع أن الإفصاح عن إدارة مخاطر الأمن السيبراني قد يؤدي إلى تخفيض عدم تماثل المعلومات وما ينتج عنه من مشكلة الاختيار المعاكس، ومن ثم يحسن من ثقة أصحاب المصالح في تلك النظم وهو ما ينعكس على قراراتهم سواء بالتقييم الإيجابي للسهم وقرار الاستثمار في الأسهم من قبل المساهمين أو التعامل على الخدمات الالكترونية للبنوك من قبل المودعين والعملاء، حيث أكدت نتائج دراسة Fisal et al. (2021) إلى أن إدارة المخاطر تسهم في تحسين القرارات الاستثمارية، وهو ما ينعكس ايجاباً على قيمة الشركات وسعر السهم.

وانطلاقاً من أن المؤسسات المالية بصفة عامة والبنوك بصفة خاصة هي أحد القطاعات الأكثر عرضة وتكراراً للمخاطر السيبرانية (الاتحاد المصري للتأمين، 2019)[14]، فإن ذلك يدعوا إلى المزيد من البحث في أثر الإفصاح عن إدارة مخاطر الأمن السيبراني في البنوك على تقييمات المستثمرين لأسهم تلك الشركات وبالتالي اتخاذ قرار الاستثمار.

فمن حيث **تأثير الإفصاح عن المخاطر بصفة عامة** فقد قدم Haddad and Alali (2022) دراسة مقارنة بين البنوك الاسلامية مقابل البنوك التجارية، وتوصلت الدراسة إلى أن هناك تأثير إيجابي معنوي بين الإفصاح

([14]) صنفت الاستراتيجية المصرية للأمن السيبراني القطاع المالي في المرتبة الثانية (من سبعة قطاعات حيوية مستهدفة للهجوم السيبراني) بعد قطاع الاتصالات وتكنولوجيا المعلومات.

عن المخاطر وكلا من مؤشري العائد على الأصول، والعائد على حقوق الملكية للبنوك الإسلامية، وفقط مع مؤشر العائد على حقوق المساهمين بالنسبة للبنوك التجارية. كما أكدت دراسة Iqbal et al. (2024) على أهمية الإفصاحات المتعلقة بإدارة المخاطر (التي يطلبها بنك التسويات الدولية من خلال معايير لجنة بازل 2015) لتقليل عدم تماثل المعلومات بين الإدارة وأصحاب المصلحة الخارجيين. وعلاوة على ذلك، فهو يزود الجهات التنظيمية ومدققي الحسابات والمحللين بمصدر جديد للمعلومات التي يمكن أن تساعدهم في تحديد البنوك المعرضة للخطر واتخاذ التدابير الوقائية للحد من التكلفة المتوقعة للفشل على الاقتصاد الكلي.

وقد أشارت دراسة Cortez and Dekker (2022) إلى أن القطاع المالي بصفة عامة، والبنوك بصفة خاصة تحولت بصورة متسارعة نحو الأنشطة الرقمية خاصة خلال فترة جائحة كورونا والعمل عن بعد، والتي أدت إلى تعرض تلك المؤسسات للمخاطر السيبرانية[15]، الأمر الذي دفع تلك المؤسسات إلى توجيه المزيد من الاهتمام نحو سياسات إدارة المخاطر السيبرانية، وظهور الحاجة من قبل أصحاب المصالح للإفصاح عن تلك المخاطر والجهود التي تتبناها الشركات لإدارتها. وترى الداسة أن أحد دوافع ذلك الإفصاح هو أنه إذا كان من الصعب على الإدارة تقديم قياساً للجهود التي تبذل لإدارة المخاطر السيبرانية، فإنه من السهل تجنيبها المسئولية في حال حدوث اختراقات، وذلك من خلال الإفصاح المسبق عن اتخاذها ما يلزم لإدارة تلك المخاطر، خاصة في ظل عدم قدرة الطرف الأخر على مراقبة جهود وتصرفات الإدارة فيما يتعلق بعملية إدارة المخاطر السيبرانية، ويتمشى ذلك مع تفسيرات **نظرية الوكالة**.

وعلى الرغم من تناول العديد من الدراسات أثر الإفصاح عن إدارة الأمن السيبراني على قرارات المستثمرين، إلا أن تلك الدراسات لم تأخذ في الاعتبار شكل ذلك الإفصاح ومحتواه، وبالتالي الأمر يتطلب البحث حول تأثير بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني، على أحكام أصحاب المصالح. فالإفصاح عن إدارة المخاطر يختلف من شركة إلى أخرى من حيث محتواه وطبيعته وكيفية التقرير عنه (شرف، 2023).

وقد أشارت الدراسات السابقة إلى أن اختلاف شكل عرض المعلومات قد يكون له تأثير مختلف على قرارات المستخدمين (Kelton et al., 2010; Hishleifer and Teoh, 2003). ويمكن تفسير ذلك من خلال نظريتين؛ الأولى **نظرية التوافق الإدراكي** Cognitive Fit [16] والتي تشير إلى أن كفاءة وفاعلية عملية اتخاذ القرار تعتمد على تحقيق التوافق بين طريقة عرض المعلومات وعملية اتخاذ القرار، إذ يحدث التوافق الإداركي عندما تكون طريقة عرض المعلومات متسقة ومدعمة لعمليات اتخاذ القرار، وعنما يحدث التوافق الإدراكي ينتج عنه تشغيل ذهني دقيق ومتسق مع طبيعة المشكلة، بما يحسن من الكفاءة والفاعلية لعملية اتخاذ القرار. أما في حالة عدم

([15]) أشارت دراسة Cortenz and Dekker (2022) إلى أن تقرير المنتدى الاقتصادي الدولي أشار إلى أن تكلفة الهجمات السيبرانية الإضافية المرتبطة بجائحة كورونا بلغت أكثر من تريليون دولار.

([16]) عرض (Kelton et al., 2010) لهذه النظرية نقلاً عن: (Verssey, 1991)

تحقيق ذلك التوافق فإن متخذ القرار قد يحتاج لتعديل طريقة عرض المعلومات ليتوافق مع طبيعة القرار، أو يعدل من عملية اتخاذ القرار (الاجراءات الذهنية) لتحقيق توافق أكبر مع طريقة عرض المعلومات، غير أن نقص التوافق الإداركي يترتب عليه زيادة في الوقت والجهد ونقص في دقة القرار (Kelton et al., 2010). أما النظرية الثانية فهي **نظرية الإدراك المحدود** Limited Attention التي قدمها Hishleifer and Teoh (2003) والتي ترى أن المستثمرين لديهم قدرة محدودة على فهم المعلومات وتشغيلها، وبالتالي فأحد النتائج المباشرة لذلك تشير إلى أن الإفصاح عن ذات المعلومات قد يكون لها آثار مختلفة على المستثمرين إذا ما تم عرضها بطرق مختلفة.

وبالتالي يقدم البحث الحالي امتداداً لذلك حيث يبحث في أهمية بدائل الإفصاح وأي منهم له تأثير على أحكام المستخدمين في أحد أهم القطاعات التي تتأثر بمخاطر الأمن السيبراني.

وعلى الرغم من إطار إعداد التقرير المالي الدولي يركز على تقديم معلومات لمقدمي التمويل بالشركات (المستثمرين والدائنين الحاللين والمحتملين)، إلا أن فئة العملاء في البنوك تعد مصدراً هاماً للتمويل إذ يمكن ادراجهم ضمن فئة الدائنين أيضاً بالقوائم المالية للبنوك، فعملاء البنوك هم محور الاهتمام في هذا النشاط الفريد، إذ أنهم المصدر الرئيسي للتمويل، والمصدر الرئيسي لتحقيق الإيرادات. فبمراجعة القوائم المالية لبعض البنوك المقيدة بالبورصة المصرية وجد الباحث أن ودائع العملاء تمثل في المتوسط 93% من إجمالي الالتزامات، وتمثل 89% من إجمالي الالتزامات وحقوق الملكية، بمعنى أن العملاء بالبنوك هم المصدر الرئيسي للتمويل (89% من إجمالي التمويل).

ووفقاً **لنظرية أصحاب المصالح**، فإن أصحاب المصلحة بالشركة يمثلون مجموعة أوسع من مستخدمي القوائم المالية مقارنة بالمساهمين والدائنين (على سبيل المثال، العملاء والحكومة)، وبالتالي فإن الشركات مطالبة بأن تكون أكثر شفافية تجاه أصحاب المصلحة، وتفترض نظرية أصحاب المصلحة أن الحفاظ على الثقة المتبادلة والتعاون مع جميع أصحاب المصلحة هو استراتيجية عمل تقلل من تكاليف التعاقد والتي تشمل الدعاوى القضائية التي يرفعها أصحاب المصلحة نتيجة لانتهاك الأمن السيبراني، ويحد من عدم التأكد الذي يمكن أن يؤدي إلى خسارة العملاء (Jaing et al., 2022). لذلك، يمكن أن يقدم الإفصاح عن إدارة المخاطر السيبرانية معلومات قد تساعد العملاء في تقييم الخسائر الحالية والمستقبلية الناجمة عن حدوث الاختراق وما إذا كانوا سيواصلون علاقتهم مع البنك، وهو ما تسعى الدراسة لاختباره. وفي حدود علم الباحث لم تتطرق أي من الدراسات السابقة لاختبار تلك الفرضية.

وبالتالي يمكن صياغة فرض الدراسة الأول على النحول التالي:

H1: تؤثر بدائل إفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني معنوياً على على أحكام عملائها والمستثمرين في أسهمها

وسيتم اختبار هذا الفرض من خلال الفروض الفرعية التالية:

H1–a: يؤثر إفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة معنوياً على أحكام عملائها والمستثمرين في أسهمها.

H1–b: يؤثر إفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل معنوياً على أحكام عملائها والمستثمرين في أسهمها.

تحليل إضافي:

يختبر الفرضين السابقين أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام المتعاملين بصورة منفصلة لكل بديل من بديلي الإفصاح محل الاختبار، لكن يبقى تساؤل هام وهو أي من بديلي الإفصاح له تأثير أكبر على أحكام المتعاملين، وبالتالي يتطلب الأمر اختبار الفرض التالي:

H1–c يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرين في أسهمها باختلاف بدائل الإفصاح.

2-10 أثر اختلاف جنس المستفيدين على تأثير الإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام المستفيدين، وتطوير فرض الدراسة الثاني.

أيدت العديد من الدراسات السابقة أن جنس المستثمرين له تأثير هام على قرارات الاستثمار (Metawa et al, 2019)[17]. وقد يرجع تأثير الجنس على قرارات الاستثمار إلى العديد من العوامل التي قدمتها الدراسات السابقة مثل الأعراف المجتمعية، والاختلافات السلوكية، والقدرة على الحصول على الموارد المالية (Shah, 2023)، غير أنه من أهم تلك العوامل التي أيدتها الدراسات السابقة تتمثل في ميل الاناث لتجنب المخاطر والضغوط المالية مقارنة بالرجال (Niessen and Zimmerer, 2024; Shaikh et al. 2019; Shah, 2023) حيث عادة ما يكون النساء أكثر تحفظاً بشأن قرارات الاستثمارات والاحتفاظ بمحفظة استثمار أقل مخاطرة مقارنة بالرجال. وقد قدمت دراسة Siraji et al. (2021) دليلاً على وجود أثر معدل للجنس على العلاقة بين السلوكيات غير الرشيدة للمستثمرين وقرارات الاستثمار، حيث خلصت الدراسة إلى أن المستثمرات يظلن متمسكات بوجهات نظرهن القديمة، ويتوقعن اتجاها مماثلا في المستقبل يقودهن إلى القرار الخاطئ. وتشير النتائج إلى أن الإناث تملن إلى اتباع المستثمرين الآخرين في قرار الاستثمار. كما توصلت دراسة شرف (2023) إلى وجود تأثير معنوي للجنس على العلاقة بين الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات المستثمرين غير المحترفين.

([17]) على الرغم من أن تلك الدراسة أشارت إلى أن هناك عوامل أخرى تتداخل مع تأثير الجنس وتؤثر في قرار الاستثمار مثل احتمالية الميراث المتوقع للإناث، عمل المرأة وصافي ثروتها، وأما بالنسبة للرجال فبعض العوامل مثل عمر الرجال، ودرجة تقبله للمخاطر، والحالة الاجتماعية، ومستوى التعلم الجامعي.

وفي سياق أخر توصلت دراسة Luo and Salterio (2022) إلى أن التفاعل بين المستثمرين من الإناث ونصيحة المحللات من الإناث تكون أكبر من أي تفاعلات أخرى يكون طرفها الذكور، وبالتالي فإن الجنس يكون له تأثير على الكيفية التي تتخذ بها قرارات الاستثمار، وأنه لا يمكن الإدعاء بتحييد عامل النوع في تأثيراته على قرارات الاستثمار.

ويمكن التوقع أيضاً بأثر الجنس قد يكون له تأثير على قرارات عملاء البنوك للتعامل على الخدمات الالكترونية للبنك، حيث قد تتأثر القرارات بمدى تقبل العملاء للمخاطر، وحيث أن الإناث أكثر ميلاً لتجنب المخاطر فمن المتوقع أن تتأثر علاقة الإفصاح عن إدارة مخاطر الأمن السيبراني وقرار التعامل على الخدمات الالكترونية للبنك بجنس المشاركين. إضافة إلى ما استخلصته دراسة Yuen (2013) من بعض الدراسات السابقة فيما يتعلق باستخدام الخدمات المصرفية الالكترونية، بأن الإناث أكثر انشغالاً بحياة الأطفال، وأقل اهتماماً باستخدام الإنترنت، وأن الرجال يشكلون غالبية مستخدمي الخدمات المالية عبر الإنترنت (76%) في البلدان الأوروبية، وأن الإناث لا ينظرن إلى الخدمات المصرفية عبر الإنترنت على أنها مفيدة مثل الذكور، غير أن ذلك قد يختلف باختلاف العوامل الثقافية بكل دولة (Yuen, 2013). كما أشار Friedman and Lowengart (2016) إلى أن فهم الاختلافات بين الذكور والإناث حول الخدمات المصرفية أمر بالغ الأهمية لنجاح البنك. وقد أشارت دراسة Zwane et al. (2023) كنتيجة لتحليل الدراسات السابقة إلى اختلاف سلوك مستخدمي الخدمات المصرفية ما بين الذكور والإناث، فالذكور يتحركون بشكل أسرع خلال مراحل التبني التكنولوجي مقارنة بالإناث، وبالتالي قد يكون الإناث أقل ميلًا لتجربة التطورات التكنولوجية الجديدة، كما أن مواقف الذكور تجاه تبني التكنولوجيا تتحدد بمدى فائدة الابتكار الذي يرونه، بينما تفضل الإناث معرفة مدى سهولة استخدامه، وقد ترجع الأسباب الرئيسية لعدم مشاركة المرأة في التكنولوجيا إلى الظروف غير المواتية التي تواجهها، مثل البطالة ونقص التعليم والدخل، وعندما يتم عكس هذه الظروف غير المواتية، قد تميل النساء إلى أن تكون أكثر انفتاحاً لاستخدام التطبيقات الرقمية، وأظهرت الدراسات السابقة إن مشاركة الإناث في الدول النامية أقل من الرجال فيما يتعلق بالاستخدامات التكنولوجية، غير أن المزيد من الوصول إلى العمل والتعليم والدخل يؤدي إلى زيادة استخدام الإناث للتكنولوجيا مثل الخدمات المصرفية عبر الإنترنت، غير أن دراسة Zwane et al. (2023) التي اجريت على دولة سوازيلاند الافريقية لم تجد فرقاً معنوياً بين الذكور والإناث نظراً لحداثة الخدمات المصرفية الالكترونية بالنسبة لكلا الجنسين، ولكن لم يكن أي من الجنسين مرتاحاً وراضياً تماماً عن استخدام الأنظمة المصرفية عبر الإنترنت الحالية.

إن فهم الدور الذي يلعبه جنس العميل في استخدام الخدمات المصرفية عبر الإنترنت يمكن أن يساعد البنوك والمؤسسات المالية في تطوير الاستراتيجيات التي يمكن أن تعزز وتشجع استخدامها (Elena-Bucea et al. 2021). فجنس العميل يعد من العوامل الهامة في دراسة الخدمات المصرفية البنكية، لأنه يُعتقد أن يكون للذكور والإناث مواقف وسلوكيات المختلفة عندما يتعلق الأمر باستخدام التكنولوجيا، وبالتالي هناك حاجة إلى مزيد من

البحث حول كيفية تأثير الجنس على استخدام الخدمات المصرفية عبر الإنترنت في البلدان النامية (Zwane et al., 2023)، وبالتالي فإن هناك حاجة إلى استكشاف الأثر المعدل للجنس على تأثير الإفصاح عن إدارة مخاطر الأمن السيبراني على تقبل عملاء البنوك للتعامل على الخدمات الاكترونية للبنك.

وبالتالي يمكن صياغة فرض الدراسة الثاني على النحو التالي:

H2: يختلف التأثير المعنوي لبدائل إفصاح البنوك في مصر عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس

ويتم اختبار ذلك الفرض من خلال الفروض الفرعية التالية:

H2-a: يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير مجلس الإدارة على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس

H2-b: يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير منفصل على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس

تحليل إضافي:

كما تم عمل تحليل إضافي للفرض الأول باختبار أي من بدائل الإفصاح أكثر معنوية في تأثيره على أحكام المشاركين، لذا يتطلب الأمر اختبار أثر الجنس على ذلك التأثير وهو ما يتم اختباره من خلال الفرض الفرعي التالي:

H2-c: تختلف معنوية تاثير بدائل إفصاح البنوك في مصر عن إدارة المخاطر السيبرانية على قرارات عملائها والمستثمرين في أسهمها باختلاف الجنس.

10-3 أثر العمر على تأثير الإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام المستفيدين، وتطوير فرض الدراسة الثالث.

أشارت العديد من الدراسات إلى تأثير العمر على قرارات المستثمرين، وأيضاً قرارات عملاء البنوك في التعامل مع الخدمات الالكترونية للبنوك، فقد وجدت دراسة Korniotis and Alok Kumar (2011) أن قرارات محفظة المستثمرين الأكبر سنا تعكس معرفة أكبر بالاستثمار، غير أن تلك القدرة تتدهور مع التقدم في السن، وقد أيدت نتائج دراستي (Metawa et al., 2019; Obamuyi, 2013) ذلك حيث توصلتا إلى وجود تأثير معنوي لكل من السن التأهيل العلمي على قرارات الاستثمار في الأسهم. كما توصلت دراسة Jain and Mandot (2021) إلى وجود علاقة معنوية بين عمر المستثمرين والقدرة على تقبل مخاطر الاستثمار.

كما اتفق عدد من الدراسات مثل (Yuen, 2013; Izogo et al., 2012; Agarwal et al., 2009؛ محمد، 2021) على أن العمر أحد العوامل الهامة التي لها تأثير معنوي على تبني الخدمات المصرفية الالكترونية.

وبناء على ذلك يمكن صياغة فرض الدراسة الثالث على النحو التالي:

H3: يختلف التأثير المعنوي لبدائل إفصاح البنوك في مصر عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف العمر

ويتم اختبار ذلك الفرض من خلال الفروض الفرعية التالية:

H3-a: يختلف التأثير المعنوي لإفصاح البنوك عن إدارة المخاطر السيبرانية من خلال تقرير مجلس الإدارة على أحكام عملائها والمستثمرين في أسهمها باختلاف العمر

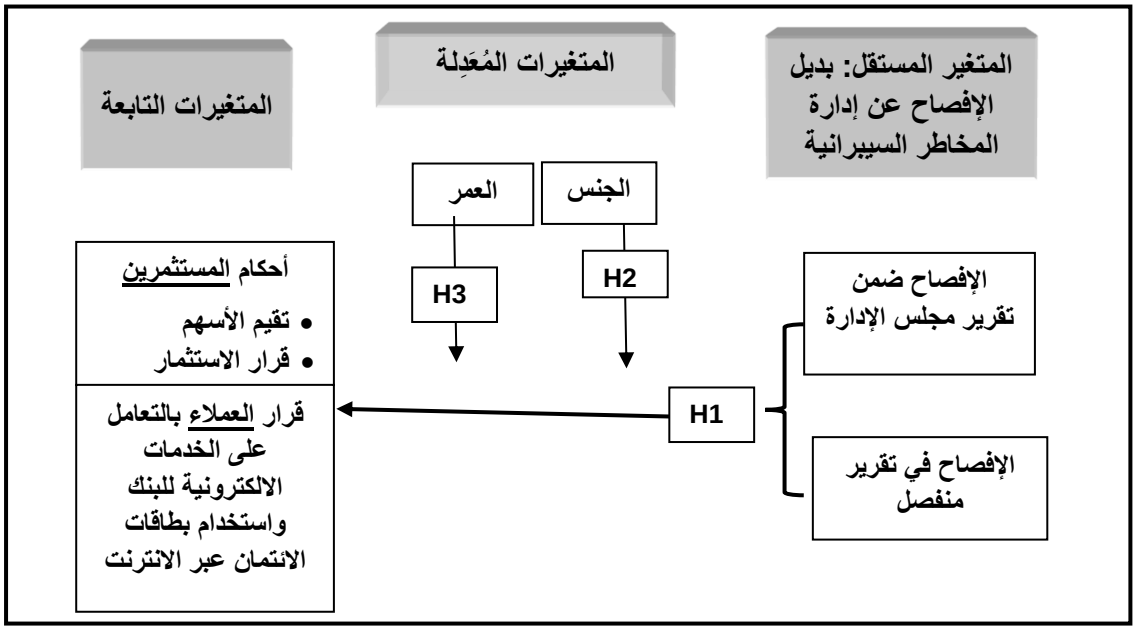
H3-b: يختلف التأثير المعنوي لإفصاح البنوك عن إدارة المخاطر السيبرانية من خلال تقرير منفصل على أحكام عملائها والمستثمرين في أسهمها باختلاف العمر

<u>تحليل إضافي:</u>

كما تم عمل تحليل إضافي للفرض الأول باختبار أي من بدائل الإفصاح أكثر معنوية في تأثيره على أحكام المشاركين، لذا يتطلب الأمر اختبار أثر العمر على ذلك التأثير وهو ما يتم اختباره من خلال الفرض الفرعي التالي:

H3-c: تختلف معنوية تاثير بدائل إفصاح البنوك في مصر عن إدارة المخاطر السيبرانية على قرارات عملائها والمستثمرين في أسهمها باختلاف العمر

ويوضح الشكل التالي نموذج لفروض بالبحث:



شكل 4: نموذج البحث

من إعداد الباحث

11- الدراسة التجريبية:

تستهدف الدراسة التجريبية اختبار أثر بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني على كل من أحكام المستثمرين والتي تتضمن تقديراتهم بشأن أسعار الأسهم وقرار الاستثمار، وأحكام عملاء البنك والمتعلقة بالتعامل على الخدمات الالكترونية للبنك. ثم اختبار أثر الجنس والعمر على العلاقة السابقة. ثم يختبر البحث الفرق بين أحكام أكاديميين المهنيين في تلك العلاقات.

11-1 مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في المحللين الماليين ومديري الاستثمار بمصر حيث تم توزيع الحالة التجريبية الكترونياً على عدد 299 مشاهدة على موقع Linked In، وعبر البريد الالكتروني، ورسائل على WhatsApp حيث تم اختيار المفردات ذات التخصص الوظيفي محلل مالي، ومدير استثمار قياساً على دراسة Reimsbach and Hahn (2017)، ولغرض اختبارات الحساسية تم توزيع الحالة التجريبية عدد 116 من أعضاء هيئة التدريس بالجامعات المصرية، لاختبار أراء الأكاديميين مقارنة بالمهنيين. وتم استبعاد المشاهدات التي لم تجتاز السؤالين الاختباريين بالتجربة. وقد تم تقسيم تلك المفردات إلى مجموعتين حصلت كلتاهما على التقارير السنوية المرفق بها تقرير مجلس الإدارة دون الإفصاح عن إدارة المخاطر السيبرانية، كمرحلة أولى، ثم في المرحلة الثانية تم تقديم تقرير مجلس الإدارة متضمناً الإفصاح عن إدارة مخاطر الأمن السيبراني للمجموعة الأولى (Group 1)، أما المجموعة الثانية (Group 2) فحصلت على تقرير منفصل يتعلق بإدارة مخاطر الأمن السيبراني، وذلك اعتماداً على التصميم التجريبي قبل-بعد المعالجة قياسا على (عثمان، 2023؛ علي وعلي، 2021 Mauldin and Arunachalam, 2002). ويوضح جدول رقم (1) عينة الدراسة:

جدول 1: عينة الدراسة

		عدد الحالات الموزعة	عدد الحالات الصحيحة المستلمة	نسبة الاستجابة
المهنيين	المجموعة التجريبية الأولى	158	62	%39
	المجموعة التجريبية الثانية	141	53	%37
الإجمالي		299	115	%38
الأكاديميين	المجموعة التجريبية الأولى	59	40	%68
	المجموعة التجريبية الثانية	57	43	%77
الاجمالي		116	83	%72
الإجمالي الكلي		414	198	%48

الخصائص الديموغرافية للعينة:

جدول 2: الخصائص الديموغرافية للعينة

		ذكور	إناث	متوسط العمر
المهنيين	المجموعة التجريبية الأولى	37	25	44
	المجموعة التجريبية الثانية	31	22	42
		68	**47**	**43**
الأكاديميين	المجموعة التجريبية الأولى	14	26	46
	المجموعة التجريبية الثانية	24	19	46
		38	**45**	**46**
العينة المجمعة		**106**	**92**	**44**

11-2 متغيرات الدراسة:

11-2-1 المتغيران المستقلان:

يتمثل المتغيران المستقلان في بدائل الإفصاح عن إدارة محاطر الأمن السيبراني، وتم قياس ذلك الأثر من خلال مقارنة أحكام المستثمرين (بشأن تقييم الأسهم والاستثمار)، والعملاء (بشأن تعاملاتهم في الخدمات الالكترونية للبنك والتعامل على البطاقات الالكترونية للبنك)، وذلك في ظل بديلي الإفصاح ضمن تقرير مجلس الإدارة (من خلال المجموعة التجريبية الأولى) أو في تقرير منفصل (من خلال المجموعة التجريبية الثانية)، ويتم اختبار ذلك من خلال مجموعتين من الاختبارات؛ الأولى من خلال اجراء الاختبار على كل مجموعة تجريبية على حدة، فلكل عينة يتم اختبار مدى وجود فروق معنوية بين أحكام المشاركين قبل وبعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني (Mauldin and Arunachalam, 2002). أما المجموعة الثانية من الاختبارات فيتم مقارنة أحكام المشاركين من المجموعة الأولى (التي تسلمت الإفصاح ضمن تقرير مجلس الإدارة) مع المجموعة الثانية (التي تضمنت الإفصاح ضمن تقرير منفصل)، تمشياً مع (Shen et al. 2017; Coram, 2009; Coram et al. 2009)

وتم تصميم نموذجي الإفصاح عن مخاطر الأمن السيبراني بالحالة التجريبية على النحو التالي:

أ- بخصوص بديل الإفصاح ضمن تقرير مجلس الإدارة، تم الاستعانة بأحد تقارير مجلس إدارة أحد البنوك الأجنبية.

ب- بخصوص بديل الإفصاح ضمن تقرير منفصل تم تطوير نموذج مقترح من خلال الاستعانة بنموذج التقرير عن إدارة مخاطر الأمن السيبراني الصادر عن (AICPA, 2018).

نبذة مختصرة عن نموذج تقرير AICPA:

تم تطوير إطار إعداد تقارير شهادة الأمن السيبراني الخاص بـ AICPA **لإنشاء آلية إعداد تقارير موحدة** لتزويد المستخدمين بمعلومات مفيدة حول برنامج إدارة مخاطر الأمن السيبراني الخاص بالمنشأة لدعم اتخاذ القرارات الصحيحة والاستراتيجية. حيث يتضمن ذلك النموذج جزئيتين أساسيتين، الأولى وصفاً لطبيعة مخاطر الأمن السيبراني، وما يجب القيام به لإدارة تلك المخاطر، والجزء الثاني يتمثل في تأكيدات الإدارة بشأن سلامة الإجراءات والسياسات التي تتبعها لإدارة تلك المخاطر. حيث:

أ- **الجزء الأول:** هو وصف مكتوب Narrative تعده الإدارة لبرنامج إدارة مخاطر الأمن السيبراني الخاص بالشركة (الوصف). ويتم تصميم هذا الوصف لتوفير معلومات حول كيفية تحديد الشركة للمعلومات الأكثر حساسية، والطرق التي تدير بها الشركة مخاطر الأمن السيبراني التي تهددها، والسياسات والعمليات الأمنية الرئيسية التي يتم تنفيذها وتشغيلها لحماية أصول معلومات الشركة من تلك المخاطر. ويوفر الوصف المحتوى

التقريري الذي يحتاجه المستخدمون لفهم الاستنتاجات التي عبرت عنها الإدارة حول فعالية الضوابط المضمنة في برنامج إدارة مخاطر الأمن السيبراني الخاص بالشركة.

ب- **تأكيد الإدارة: حيث** تقدم الإدارة تأكيدًا حول ما إذا كان الوصف قد تم تقديمه وفقًا لمعايير الوصف وما إذا كانت أدوات الرقابة داخل البرنامج فعالة لتحقيق أهداف الأمن السيبراني للشركة.

ويرى AICPA (2018) أن إطار إعداد التقارير المقدم عن إدارة مخاطر الأمن السيبراني هو خطوة أولى حاسمة لتمكين حل متسق للشركات للتواصل بشكل فعال مع أصحاب المصلحة الرئيسيين حول كيفية إدارة مخاطر الأمن السيبراني. مع زيادة نضج برامج إدارة مخاطر الأمن السيبراني في الشركات، يمكن لإطار إعداد التقارير أيضًا أن يكون بمثابة الأساس لخدمات تصديق عالية الجودة على مستوى الفحص، والتي يؤديها محاسب قانوني معتمد مستقل.

11-2-2المتغير التابع:

11-2-2-1 أحكام المستثمرين في الأسهم:

أ- توقعات المستثمر بشأن سعر السهم المستقبلي: ويتم قياسه من خلال متغير ترتيبي يأخذ قيمة من 1 إلى 5 حيث تعبر القيمة (1) عن توقعات المستثمر بانخفاض شديد في سعر السهم، والقيمة (2) توقعات بانخفاض محدود في سعر السهم، والقيمة (3) تعبر عن استقرار سعر السهم، القيمة (4) تعبر ارتفاع محدود في سعر السهم، والقيمة (5) تعبر عن ارتفاع كبير في سعر السهم، قياساً على (كعموش، 2018).

ب- قرار الاستثمار في اسهم الشركة: ويتم قياسه من خلال متغير ترتيبي يأخذ قيمة من 1 إلى 5 والذي يعبر عن احتمال شراء المستثمر لأسهم الشركة (علي وعلي، 2021). حيث تأخذ القيمة (1) إذا كان احتمال الشراء أقل من 25%، القيمة (2) إذا كان الاحتمال أكبر من 25% وأقل من 50%، القيمة (3) تعبر عن الاحتمال المحايد 50%، القيمة (4) تعبر عن احتمال الشراء أكبر من 50% وحتى 75%، والقيمة (5) تعبر عن احتمال الشراء أكبر من 75%، قياساً على (عثمان، 2023؛ كعموش، 2018).

11-2-2-2 أحكام العملاء:

قرار التعامل في الخدمات الالكترونية المصرفية وبطاقات الائتمان للشراء عبر الانترنت. ويتم قياسه من خلال اعطاء المشارك درجة من 1-10 (قياساً على شرف، 2023)، تعبر عن رأيه في احتمال تعامله على الخدمات المصرفية للبنك، واستخدام البطاقات الائتمانية للشراء عبر الانترنت. حيث تأخذ القيمة (1) عدم رغبته في التعامل الالكتروني، بينما تأخذ القيمة (10) رغبته الكاملة في التعامل الالكتروني.

11-2-3 المتغيرات المعدلة:

أ- الجنس: ويتم قياسه من خلال متغير ثنائي يأخذ القيمة (1) للمشاركين الذكور، والقيمة (صفر) للمشاركين النساء (محمد 2021؛ Yuen, 2013).

ب- العمر: وقد قام الباحث باحتساب متوسط عمر المشاركين على مستوى العينة كل وكانت 44 سنة، وبناءً عليه تم تقسيم المتغير إلى فئتي، الأكبر سناً من هم من 44 سنة فأكثر، والأقل سناً من هم دون 44 عاماً (Yuen, 2013). وعلى الرعم من أن العمر متغير متصل، إلا أن الكثير من الدراسات التجريبية التي تستخدم الاختبارات اللامعلمية تقوم باستخدام المقياس الثنائي لتلك المتغيرات (علي وعلي، 2022؛ كعموش، 2018، موسى 2018) إذ أن تقسيم المتغيرات المعدلة في الاختبارات اللامعلمية لعدد من المستويات سيتطلب تقسيم العينة إلى عدد من العينات الفرعية بحسب عدد مستويات ذلك المتغير، وهو ما لا يمكن تطبيقه في الدراسة عملياً لمحدودية عينة الدراسة. ويعد ذلك قيداً على النتائج التي يمكن الوصول إليها والمتعلقة بأثر العمر، وهو ما يجب أن تؤخذ النتائج في ضوئه.

11-3 التصميم التجريبي:

تم تقسيم عينة الدراسة إلى مجموعتين أساسيتين، المجموعة الأولى لاختبار أثر بديل الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة، والمجموعة الثانية لاختبار أثر بديل الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال التقرير المنفصل. ومرت الحالة التجريبية بمرحلتين لكل مجموعة من مجموعتي الدراسة على النحو التالي:

المرحلة الأولى: حصلت المجموعتين على التقارير المالية متضمنة القوائم المالية، وجزء من تقرير مجلس الإدارة بشأن إدارة المخاطر بصفة عامة، دون تقديم الإفصاح عن إدارة المخاطر السيبرانية.

ثم قدمت مجموعة من الأسئلة للوقوف على رأي المشارك كمستثمر وقراره بشأن تقييم السهم وقرار الاستثمار، ثم رأيه كعميل بشأن التعامل مع خدمات البنك الالكترونية واستخدام بطاقات الائتمان في الشراء عبر الانترنت.

وقبل بدء المرحلة الثانية تم اخبار المشاركين بعدم إمكانية تعديل إجاباتهم السابقة اعتماداً على المعلومات التي ستقدم لهم في المرحلة الثانية.

المرحلة الثانية: تم اخبار المشاركين في التجربة بأنه بفرض أن الشركة قدمت الإفصاح الملحق بالقوائم المالية، حيث استلمت المجموعة الأولى تقرير مجلس الإدارة (يتضمن الإفصاح عن إدارة مخاطر الأمن السيبراني)، واستلمت المجموعة الثانية تقرير منفصل عن إدارة الأمن السيبراني. وطلب منهم اتخاذ قرار بشأن تقييمهم للسهم والاستثمار فيه كمستثمرين، وقرار التعامل في الخدمات الالكترونية للبنك كعملاء.

ولاختبار فروض الدراسة تم استخدام تصميم تجريبي (4 × 2 × 2) ويوضح الجدول التالي التصميم التجريبي:

جدول 3: التصميم التجريبي

م. معدلة / م. مستقلة	سمات متخذ القرار			
	الجنس		العمر	
	ذكور	اناث	أكبر من المتوسط	أقل من المتوسط
الإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة (مجموعة 1)	قرارات المشاركين رقم (9)	قرارات المشاركين رقم (10)	قرارات المشاركين رقم (11)	قرارات المشاركين رقم (12)
الإفصاح عن إدارة مخاطر الأمن السيبراني بتقرير منفصل (مجموعة 2)	قرارات المشاركين رقم (13)	قرارات المشاركين رقم (14)	قرارات المشاركين رقم (15)	قرارات المشاركين رقم (16)
عدم الإفصاح عن مخاطر الأمن السيبراني (مجموعة 1)	قرارات المشاركين رقم (1)	قرارات المشاركين رقم (2)	قرارات المشاركين رقم (3)	قرارات المشاركين رقم (4)
عدم الإفصاح عن مخاطر الأمن السيبراني (مجموعة 2)	قرارات المشاركين رقم (5)	قرارات المشاركين رقم (6)	قرارات المشاركين رقم (7)	قرارات المشاركين رقم (8)

قرارات المشاركين رقم (1، 2، 3، 4): تشمل أحكام المشاركين في المجموعة التجريبية الأولى قبل حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني.

قرارات المشاركين رقم (5، 6، 7، 8): تشمل أحكام المشاركين في المجموعة التجريبية الثانية قبل حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني.

قرارات المشاركين رقم (9، 10): تشمل قرارات المشاركين في المجموعة التجريبية الأولى بعد حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة من **الذكور والإناث على التوالي.**

قرارات المشاركين رقم (11، 12): تشمل قرارات المشاركين في المجموعة التجريبية الأولى بعد حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة من **الأكبر سناً والأصغر سناً على التوالي.**

قرارات المشاركين رقم (13، 14): تشمل قرارات المشاركين في المجموعة التجريبية الثانية بعد حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل من **الذكور والإناث على التوالي.**

قرارات المشاركين رقم (15، 16): تشمل قرارات المشاركين في المجموعة التجريبية الثانية بعد حصولهم على الافصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل من **الأكبر سناً والأصغر سناً على التوالي.**

وبذلك تكون اختبارات الفروض على النحو التالي:

اختبار فرض الدراسة الأول (H1-a): (تصميم 2× 1) اختبار قبلي- بعدي:

يتم مقارنة قرارات المشاركين في المجموعة التجريبية الأولى بدون الإفصاح عن إدارة مخاطر الأمن السيبراني مقابل أحكامهم بعد الإفصاح عن مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة (1+2+3+4) × (9 + 10 + 11 + 12).

اختبار فرض الدراسة الأول (H1–b): (تصميم 2× 1) اختبار قبلي– بعدي:

يتم مقارنة قرارات المشاركين في المجموعة التجريبية الأولى بدون الإفصاح عن إدارة مخاطر الأمن السيبراني مقابل أحكامهم بعد الإفصاح عن مخاطر الأمن السيبراني (5+6+7+8)×(13+14+15+16)

اختبار فرض الدراسة الأول (H1–c): (تصميم 2× 1) (Between Groups)

يتم مقارنة قرارات المشاركين في المجموعة التجريبية الأولى بعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة بقرارات المشاركين في المجموعة التجريبية الثانية بعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل (9+10+11+12)×(13+14+15+16).

اختبار فرض الدراسة الثاني (H2–a): (تصميم 2× 2) اختبار قبلي– بعدي:

حيث يتم: مقارنة قرارات **المجموعة التجريبية الأولى** من **الذكور** (قبل الإفصاح مقابل بعد الافصاح **ضمن تقرير مجلس الإدارة)**، مقابل قرارات نفس المجموعة **من الإناث** [(9)×(1)] × [(10)×(2)]

اختبار فرض الدراسة الثاني (H2–b): (تصميم 2× 2) اختبار قبلي– بعدي:

اختبار قرارات المجموعة **التجريبية الثانية** من **الذكور** (قبل الإفصاح مقابل بعد الإفصاح **ضمن تقرير منفصل)**، مقابل قرارات نفس المجموعة من **الإناث** [(13)×(5)] × [(14)×(6)].

<u>تحليل إضافي:</u> اختبار الفرق بين قرارات الذكور والإناث للمشاركين بعد الحصول على الافصاح ضمن تقرير مجلس الادارة مقارنة بالافصاح في تقرير مستقل (H2–c) [(9)×(13)] × [(10)×(14)]

اختبار فرض الدراسة الثالث (H3–a): (تصميم 2× 2) اختبار قبلي– بعدي:

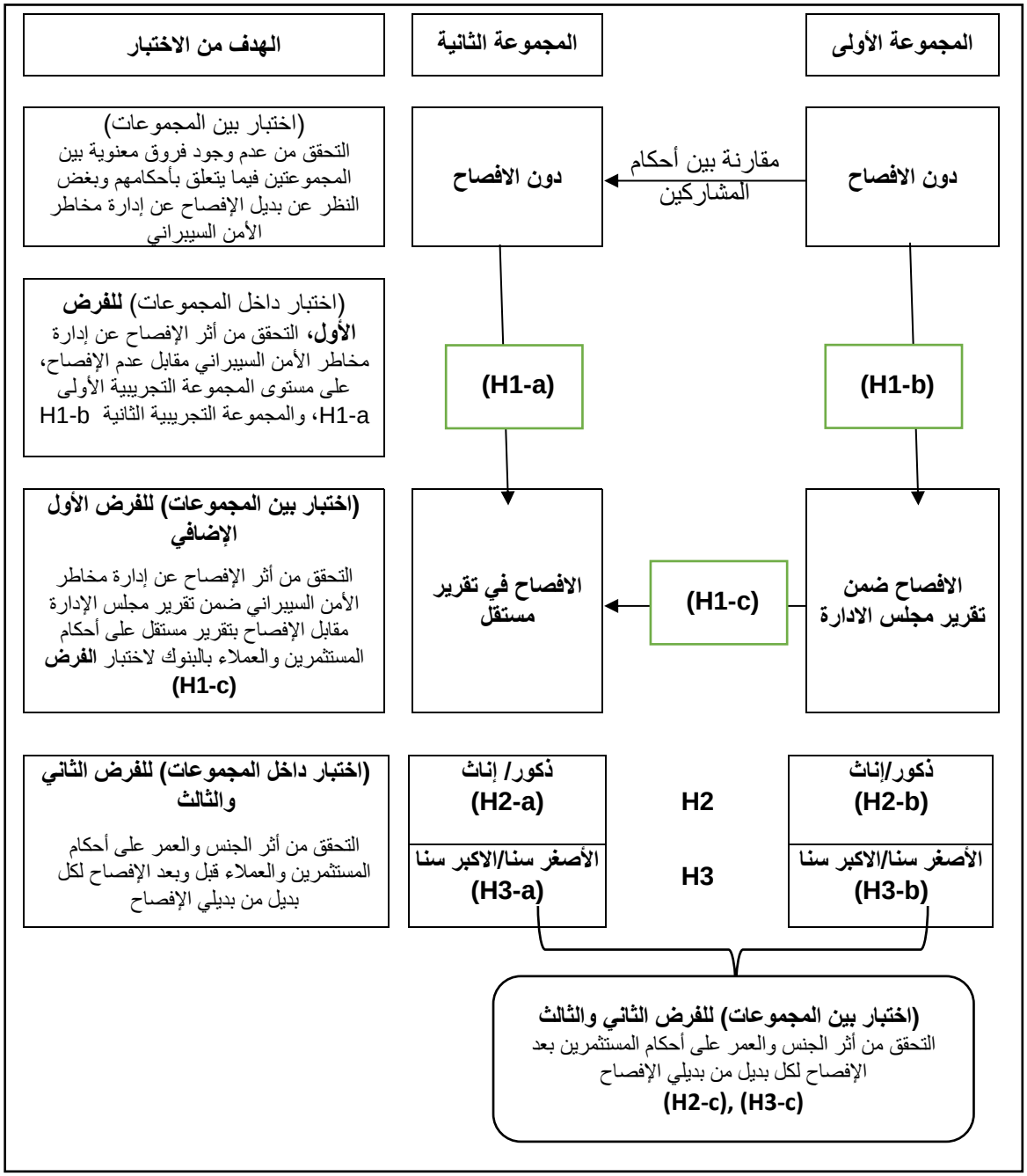
حيث يتم: مقارنة قرارات **المجموعة التجريبية الأولى** من **الأكبر سناً** (قبل الإفصاح مقابل بعد الافصاح **ضمن تقرير مجلس الإدارة)**، مقابل قرارات نفس المجموعة **من الأصغر سناً** [(11)×(3)] × [(12)×(4)].

اختبار فرض الدراسة الثاني (H3–b): (تصميم 2× 2) اختبار قبلي– بعدي:

اختبار قرارات المجموعة **التجريبية الثانية** من **الأكبر سناً** (قبل الإفصاح مقابل بعد الإفصاح **ضمن تقرير منفصل)**، مقابل قرارات نفس المجموعة من **الأصغر سناً** [(15)×(7)] × [(16)×(8)].

<u>تحليل إضافي:</u> اختبار الفرق بين قرارات الأكبر سناً والأقل سناً للمشاركين بعد الحصول على الافصاح ضمن تقرير مجلس الادارة مقارنة بالافصاح في تقرير مستقل (H3–c) [(11)×(15)] × [(12)×(16)]

وبذلك يمكن توضيح تصميم الاختبارات الاحصائية الأساسية والإضافية على النحو التالي:



شكل 5: تصميم الاختبارات الاحصائية

من إعداد الباحث

ويعتقد الباحث أن ذلك التصميم التجريبي يحقق العديد من المنافع منها:

أ- يتيح هذا التصميم مقارنة وجود فروق معنوية بين قرارات المشاركين قبل عرض نموذج الإفصاح عن إدارة مخاطر الأمن السيبراني، على مستوى جميع المشاركين في التجربة بما يؤدي إلى التحقق من عدم وجود أي فروق في القرارات ناتجة عن وجود فرق معنوي بين المجموعتين.

ب-أن تقديم الحالة التجريبية أولاً بدون الإفصاح عن إدارة مخاطر الأمن السيبراني والحصول على تقييمات المشاركين، ثم الحصول على أحكامهم مرة أخرى بعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني

يعزل أثر العوامل الأخرى التي قد تؤثر في أحكام المشاركين بخلاف الإفصاح عن إدارة مخاطر الأمن السيبراني. إضافة إلى أن التصميم المتبع في ذلك يتجنب أثر التعلم الذي يمثل أحد عيوب التصميم التجريبي قبل وبعد، حيث لم تعرض على المشاركين البيانات ذاتها مرتين وإنما ما قدم إليه في المرحلة الثانية هو الإفصاح عن إدارة مخاطر الأمن السيبراني فقط والمراد قياس أثره على أحكام المشاركين.

ج- استخدام التصميم بين المجموعات (Between groups) في الاختبارات الإضافية يستبعد أي أثر محتمل للتعلم.

إضافة إلى ما سبق قد تضمنت التجربة مجموعة من الأسئلة الاختبارية للوقوف على اتساق المشاركين في اجاباتهم، فمثلاً السؤال رقم (5) يؤكد على نتائج السؤال رقم (7)، والسؤال رقم (8) يؤكد على نتائج السؤال رقم (9)، وبالتالي فإن التناقض في نتائج تلك الأسئلة يعني عدم اتساق في اجابات المشاركين.

11-4 الاحصاء الوصفي:

يوضح الجدول رقم (4) البيانات الاحصائية لمتغيرات الدراسة لعينة المهنيين

جدول 4: الإحصاء الوصفي لمتغيرات الدراسة **على مستوى المهنيين**

المتغير (السؤال)	المجموعة التجريبية	N	Mean	Median	SD	Min	Max
1-اعتماداً على ما تقدم من معلومات، هل توافق على ان هذا البنك سيكون له أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات المنافسة	الأولى	62	6.42	6.00	1.675	3	9
	الثانية	53	4.26	5.00	2.505	1	10
	الاجمالي	115	5.43	6.00	2.351	1	10
2-إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 31 /2023/12 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي	الأولى	62	3.60	4.00	.586	2	4
	الثانية	53	3.43	3.00	.694	2	5
	الاجمالي	115	3.52	4.00	.640	2	5
3-ما هو احتمال استثمارك في أسهم تلك الشركة:	الأولى	62	3.02	3.00	.799	1	4
	الثانية	53	2.87	3.00	.735	1	4
	الاجمالي	115	2.95	3.00	.771	1	4
4- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة:	الأولى	62	5.84	5.00	1.642	3	9
	الثانية	53	6.13	5.00	2.167	3	10
	الاجمالي	115	5.97	5.00	1.899	3	10
5- هل ترى أن الإفصاح عن إدارة مخاطر الأمن السيبراني التقرير السابق الإشاره إليه يوفر لك معلومات مفيدة يمكن الاعتماد عليها عند اتخاذ قرار الاستثمار:	الأولى	62	6.94	8.00	2.141	1	10
	الثانية	53	8.28	9.00	1.714	3	10
	الاجمالي	115	7.56	8.00	2.061	1	10
6- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 31 /2023/12 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:	الأولى	62	3.87	4.00	.757	2	5
	الثانية	53	4.22	4.00	.811	2	5
	الاجمالي	115	4.03	4.00	.798	2	5
7- ما هو احتمال استثمارك في أسهم تلك الشركة:	الأولى	62	3.52	4.00	1.067	1	5
	الثانية	53	3.94	4.00	.818	2	5
	الاجمالي	115	3.71	4.00	.980	1	5
8- هل ترى أن المعلومات عن "إدارة مخاطر الأمن السيبراني" الواردة بالتقرير السابق الإشار إليه يوفر لك لك معلومات مفيدة يمكن الاعتماد عليها عند اتخاذ قرار التعامل مع البنك كأحد عملاءه؟	الأولى	62	7.05	7.00	1.945	2	10
	الثانية	53	7.43	8.00	2.126	3	10
	الاجمالي	115	7.23	7.00	2.031	2	10
9- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة التي لم تقدم معلومات حول إدارة مخاطر الأمن السيبراني؟	الأولى	62	7.32	8.00	1.818	3	10
	الثانية	53	7.11	7.00	2.276	3	10
	الاجمالي	115	7.23	8.00	2.035	3	10

من الجدول السابق يتضح أن متوسط أحكام المشاركين بعد الحصول على الإفصاح المتعلق بإدارة المخاطر السيبرانية كانت أكبر مقارنة بتلك الأحكام قبل الحصول على ذلك الإفصاح، سواءً كان ذلك على مستوى المجموعة التجريبية الأولى (التي حصلت على الإفصاح من خلال تقرير مجلس الإدارة) أو المجموعة التجريبية الثانية (التي حصلت على الإفصاح من خلال تقرير مستقل) أو حتى على المستوى الإجمالي. ويمكن ملاحظة ذلك بمقارنة سؤال 2 مقابل سؤال 6 والمرتبط بتقييم السهم، وسؤال 3 مقابل سؤال 7 والمرتبط بقرار الاستثمار في السهم، وسؤال 4 مقابل سؤال 9 والمرتبط باستخدام الخدمات الالكترونية البطاقات الائتمانية للشراء عبر الانترنت. كما أن المشاركين يرون بنسبة حوالي 70% أن الإفصاح المقدم بشأن إدارة المخاطر السيبرانية يوفر معلومات يمكن الاعتماد عليها كمدخلات لقرارات الاستثمار (س5) وقرار التعامل على الخدمات الالكترونية للبنك (س8).

جدول 5: الإحصاء الوصفي لمتغيرات الدراسة **على مستوى الأكاديميين**

المتغير (السؤال)	المجموعة التجريبية	N	Mean	Median	SD	Min	Max
1- اعتماداً على ما تقدم من معلومات، هل توافق على ان هذا البنك سيكون له أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات المنافسة	الأولى	40	6.95	7.50	1.853	3	9
	الثانية	43	6.37	6.00	2.289	1	10
	الاجمالي	83	6.65	7.00	2.098	1	10
2- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2023/12/ 31 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي	الأولى	40	3.53	4.00	.599	2	4
	الثانية	43	3.74	4.00	.581	3	5
	الاجمالي	83	3.64	4.00	.596	2	5
3- ما هو احتمال استثمارك في أسهم تلك الشركة:	الأولى	40	3.08	3.00	.888	1	4
	الثانية	43	3.30	3.00	.887	2	5
	الاجمالي	83	3.19	3.00	.890	1	5
4- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة:	الأولى	40	6.30	6.50	1.897	3	9
	الثانية	43	6.05	6.00	2.257	1	10
	الاجمالي	83	6.17	6.00	2.083	1	10
5- هل ترى أن الإفصاح عن إدارة مخاطر الأمن السيبراني التقرير السابق الإشاره إليه يوفر لك معلومات مفيدة يمكن الاعتماد عليها عند اتخاذ قرار الاستثمار:	الأولى	40	7.08	7.00	2.030	2	10
	الثانية	43	8.07	9.00	1.334	5	9
	الاجمالي	83	7.59	8.00	1.767	2	10
6- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2023/12/ 31 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:	الأولى	40	3.38	3.50	.705	2	4
	الثانية	43	4.38	5.00	.841	3	5
	الاجمالي	83	3.90	4.00	.924	2	5
7- ما هو احتمال استثمارك في أسهم تلك الشركة:	الأولى	40	3.20	3.00	.939	1	5
	الثانية	43	4.28	4.00	.766	2	5
	الاجمالي	83	3.76	4.00	1.007	1	5
8- هل ترى أن المعلومات عن "إدارة مخاطر الأمن السيبراني" الواردة بالتقرير السابق الإشار إليه يوفر لك لك معلومات مفيدة يمكن الاعتماد عليها عند اتخاذ قرار التعامل مع البنك كأحد عملاءه؟	الأولى	40	7.53	8.00	2.172	2	10
	الثانية	43	7.91	8.00	1.360	4	9
	الاجمالي	83	7.72	8.00	1.796	2	10
9- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة التي لم تقدم معلومات حول إدارة مخاطر الأمن السيبراني؟	الأولى	40	7.55	8.00	2.112	3	10
	الثانية	43	7.74	8.00	1.544	4	10
	الاجمالي	83	7.35	8.00	2.228	1	10

وكما كان الحال في عينة المهنيين، فإن الجدول رقم (5) يشير إلى نتائج متشابهة بالنسبة للأكاديميين، حيث يتضح أن متوسط أحكام المشاركين بعد الحصول على الإفصاح المتعلق بإدارة المخاطر السيبرانية كانت أكبر

مقارنة بتلك الأحكام قبل الحصول على ذلك الإفصاح، سواءً كان ذلك على مستوى المجموعة التجريبية الأولى أو المجموعة التجريبية أو حتى على المستوى الإجمالي.

ويوضح جدول رقم (6) معاملات الارتباط بين متغيرات الدراسة.

جدول 6: معاملات الارتباط بين متغيرات الدراسة

		AGE	Gender	Group	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
عينة المهنيين	AGE	1.00	.135	-.189*	.228*	.341**	.156	.297**	-.196*	.138	-.129	-.186*	-.263**
	Gender		1.00	-.012	-.057	-.131	.146	-.005	.330**	.126	.170	.403**	.314**
	Group			100	-.427**	-.147	-.091	.031	.058	.229*	.194*	.117	-.027
	Q1				1.00	.328**	.438**	.370**	.240**	.036	.157	.220*	.281**
	Q2					1.00	.620**	.122	-.027	.188*	-.011	-.076	-.041
	Q3						1.00	.332**	.220*	.410**	.577**	.273**	.240**
	Q4							1.00	.227*	.182	.069	.299**	.233*
	Q5								1.00	.774**	.768**	.432**	.881**
	Q6									1.00	.768**	.165	.155
	Q7										1.00	.313**	.342**
	Q8											1.00	.935**
	Q9												1.00
عينة الأكاديميين	AGE	1.00	.105	-.004	.326**	-.077	-.012	.090	-.043	-.164	-.102	.069	.124
	Gender		1.00	.186	-.004	-.127	-.013	.074	.081	.059	.044	.133	.183
	Group			1.00	-.130	.156	.117	-.062	-.078	.548**	.557**	-.153	-.019
	Q1				1.00	.166	.126	.820**	.254*	-.284**	-.098	.275*	.325**
	Q2					1.00	.876**	.117	-.273*	.140	.091	-.259*	-.312**
	Q3						1.00	.180	-.075	.183	.410**	-.036	.076
	Q4							1.00	.365**	-.134	.059	.377**	.502**
	Q5								1.00	.862**	.865**	.844**	.796**
	Q6									1.00	.729**	-.189	-.047
	Q7										1.00	.146	.189
	Q8											1.00	.918**
	Q9												1.00

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

يتضح من مصفوفة الارتباطات أن السؤال الثاني (والذي يتعلق بتقييم السهم) يرتبط معنوياً موجباً بالسؤال الثالث (والذي يرتبط بقرار الاستثمار) وهو ما يعبر عن منطقية استجابات المشاركين كمستثمرين سواء على مستوى عينة المهنيين، أو على مستوى الأكاديميين. كما كان هناك ارتباطاً معنوياً موجباً وقوياً بين اجابة السؤال الثامن (والذي يتعلق بمدى تقديم الإفصاح عن "إدارة مخاطر الأمن السيبراني" معلومات مفيدة يمكن الاعتماد عليها عند اتخاذ قرار التعامل مع البنك كأحد عملاءه) وبين السؤال التاسع والمتعلق برغبة العميل في التعامل مع الأنشطة والخدمات الالكترونية المقدمة من البنك. كا يلاحظ أن الارتباط بين أحكام المشاركين قبل الحصول على الإفصاح لا ترتبط معنوياً في جميع الحالات مع الأحكام المناظرة لها بعد الحصول على الإفصاح، وذلك يدل على أن الإفصاح كان له تأثيراً على أحكام المشاركين وبصورة متفاوته حيث المعاملات السابقة للارتباط تتضمن بديلي الإفصاح معاً والذي من المحتمل أن يكون لهما تأثيرات متباينة من حيث القوة أو الاتجاه على قرارات وأحكام المشاركين، وهو ما تسعى الاختبارات الإحصائية للفروض لاختباره. كما كان هناك ارتباطاً معنوياً بين السؤال الخامس (والمتعلق بمدى تقديم الإفصاح المقدم معلومات نافعة لغرض اتخاذ قرار الاستثمار) وبين السؤالين السادس

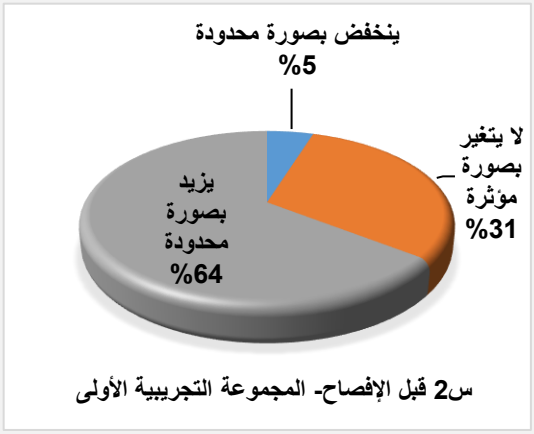
والسابع (والمرتبطين بقرارات الاستثمار) وهو ما يشير إلى منطقية واتساق استجابات المشاركين، غير أن الثبات والاتساق الداخلي سيتم اختبارها إحصائياً ضمن اختبارات العينة.

ويقدم الشكل (6) وشكل (7) ملخصاً لنسب استجابات المشاركين على الأسئلة الأساسية المستخدمة لاختبارات الفروض والتي تعبر عن أحكام المشاركين قبل وبعد الحصول على الإفصاح عن إدارة المخاطر السيبرانية، وذلك لكل مجموعة من المجموعتين التجريبيتين، حيث الأولى حصلت على الإفصاح من خلال تقرير مجلس الإدارة، بينما حصلت الثانية على الإفصاح من خلال تقرير منفصل.

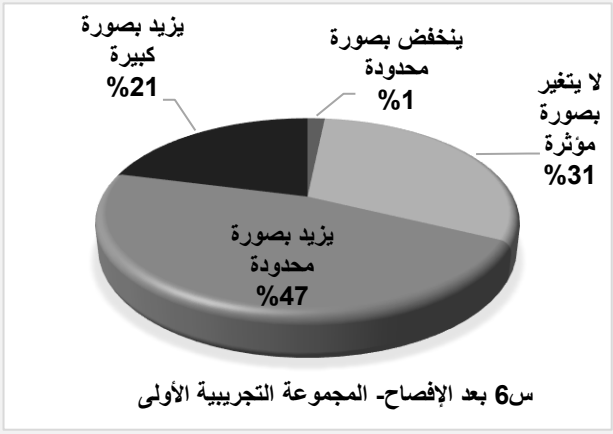
ويتضح من الشكل رقم (6) أن أحكام المستثمرين بشأن تقييم الأسهم، واتخاذ قرار الاستثمار في البنك زادت بعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإجارة، كذلك زادت رغبة المشاركين في استخدام الخدمات الالكترونية للبنك (كعملاء للبنك) بعد الحصول على ذلك الإفصاح. كما من الشكل (رقم 7) أن أحكام المستثمرين بشأن تقييم الأسهم، واتخاذ قرار الاستثمار في البنك زادت بعد الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني، كذلك زادت رغبة المشاركين في استخدام الخدمات الالكترونية للبنك (كعملاء للبنك) بعد الحصول على ذلك الإفصاح من خلال تقرير منفضل.

وتتشابه تلك الاستنتاجات في ظل بديلي الإفصاح، غير أن تلك الاستنتاجات يجب أن يتم اختبارها إحصائياً، إضافة إلى الحاجة إلى اختبار أي من بديلي الإفصاح له تأثير أكثر معنوية على أحكام المشاركين، وهو ما سيتم اختباره بصورة تفصيلية في اختبارات الفروض.

- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2023/12/31 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:

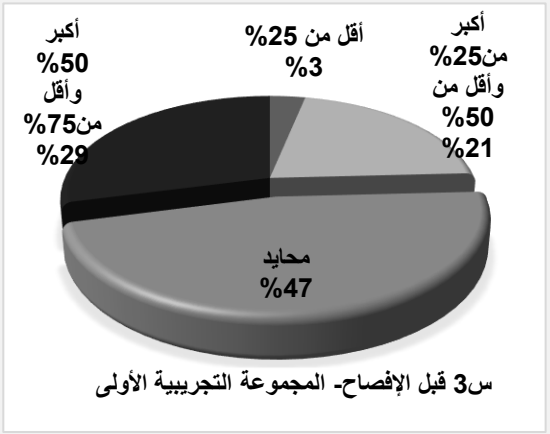


س2 قبل الإفصاح- المجموعة التجريبية الأولى

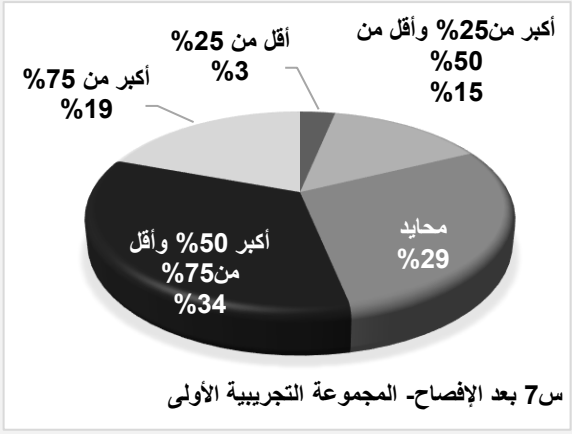


س6 بعد الإفصاح- المجموعة التجريبية الأولى

- ما هو احتمال استثمارك في أسهم شركة "بنك الحضارة"

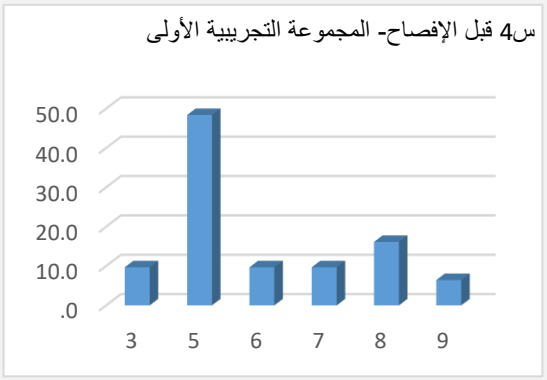


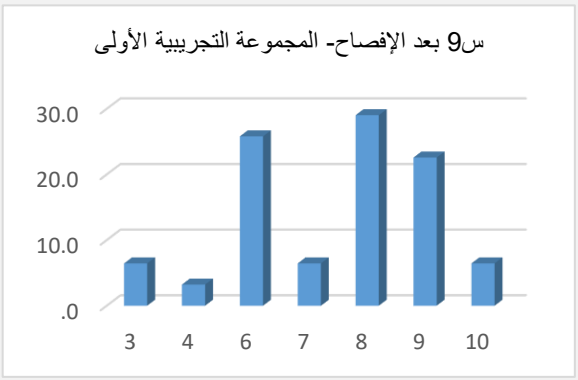
س3 قبل الإفصاح- المجموعة التجريبية الأولى



س7 بعد الإفصاح- المجموعة التجريبية الأولى

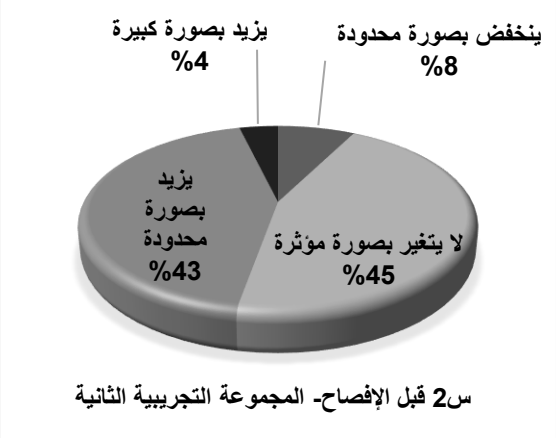
- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة:



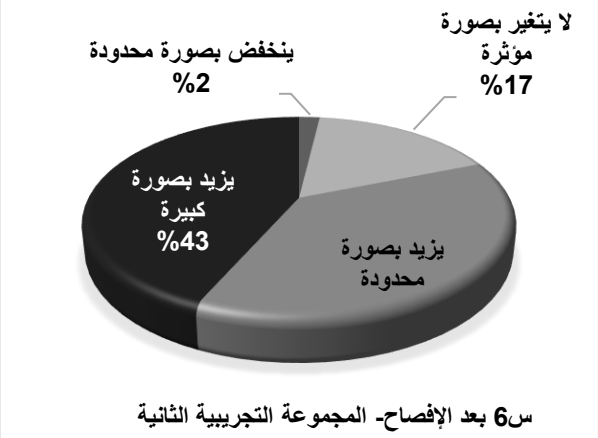


شكل رقم (6) استجابات المشاركين في عينة المهنيين لأسئلة التجربة (قبل وبعد الحصول على الإفصاح) للمجموعة التي حصلت على الإفصاح من خلال تقرير مجلس الإدارة

- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2023/12/31 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:

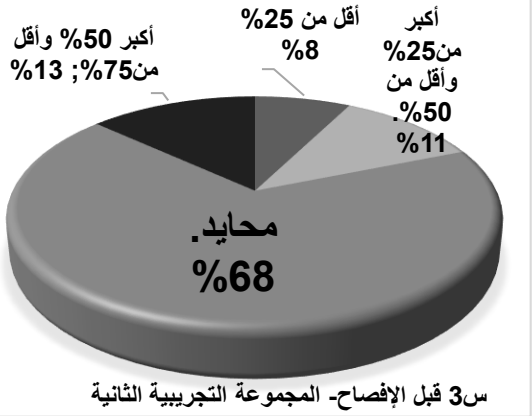


س2 قبل الإفصاح- المجموعة التجريبية الثانية

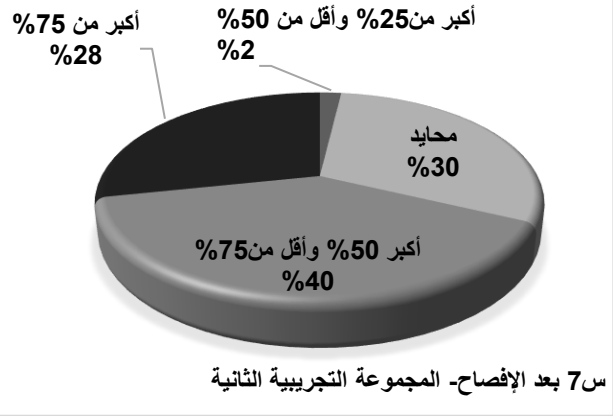


س6 بعد الإفصاح- المجموعة التجريبية الثانية

- ما هو احتمال استثمارك في أسهم شركة "بنك الحضارة"

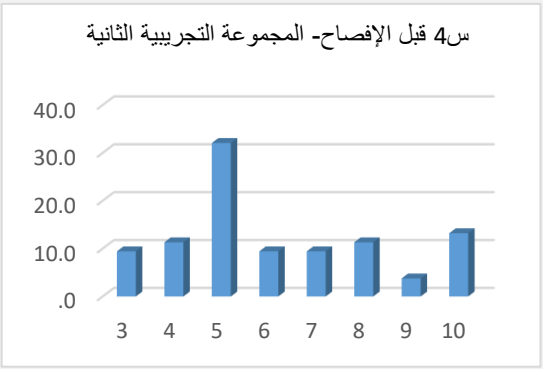


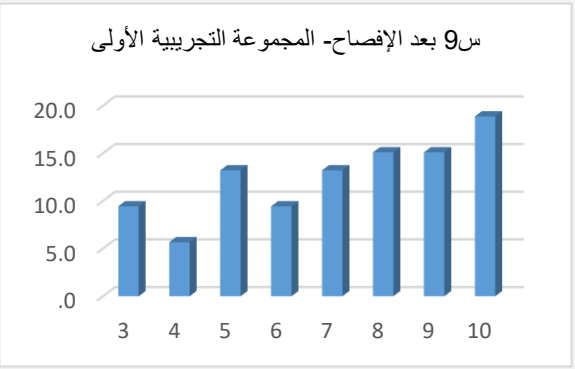
س3 قبل الإفصاح- المجموعة التجريبية الثانية



س7 بعد الإفصاح- المجموعة التجريبية الثانية

- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة:





شكل رقم (7) استجابات المشاركين في عينة المهنيين لأسئلة التجربة (قبل وبعد الحصول على الإفصاح) للمجموعة التي حصلت على الإفصاح من خلال تقرير منفصل

11-5 اختبارات العينة:

11-5-1قياس الصدق والثبات لإجابات عينتي الدراسة:

تم استخدام اختبار كرونباخ الفا لقياس مدى الثبات الداخلي وامكانية الاعتماد على اجابات المشاركين في العينة (عزام و زغلول، 2006)، فقد تم تطبيق الاختبار مع تقسيم الأسئلة المستخدمة في التجربة إلى مجموعتين من الأسئلة (4) أسئلة على مقياس ليكرت الخماسي، و(5) اسئلة على مقياس من 10 درجات ويتضح من الجدول رقم (7) أن قيمة معامل Cronbach's Alpha تجاوزت نسبة 70% سواء على مستوى العينة ككل أو على مستوى العينات الفرعية للمهنيين والأكاديميين.

جدول 7: اختبار Cronbach's Alpha للثبات وامكانية الاعتماد على إجابات العينة

	الأسئلة على القياس من 10 درجات			الاسئلة على مقياس ليكرت الخماسي		
	معامل Cronbach's Alpha	عدد العناصر	عدد المشاهدات	معامل Cronbach's Alpha	عدد العناصر	عدد المشاهدات
عينة المهنيين	.788	5	115	.767	4	115
عينة الأكاديميين	.894	5	83	.775	4	83
العينة ككل	.839	5	198	.771	4	198

11-5-2اختبار اعتدالية البيانات:

تم استخدام اختبار Kolmogorov-Smirnov لتحديد طبيعة توزيع البيانات محل الدراسة وذلك بهدف التعرف على ما إذا كان سيتم الاعتماد على الاختبارات المعلمية أو اللامعلمية لاختبار الفروض، وقد جاءت جميع قيم P-value أقل من 5% (جدول رقم 8) وبالتالي يتم عدم قبول فرض العدم القائل بأن البيانات تتبع التوزيع الطبيعي، وقبول الفرض البديل القائل بأن البيانات لا تتبع التوزيع الطبيعي، وبالتالي سيتم استخدام الاختبارات اللامعلمية.

جدول 8: اختبار إعتدالية البيانات

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.
Q2	.345	198	.000	.764	198	.000
Q3	.238	198	.000	.863	198	.000
Q4	.188	198	.000	.947	198	.000
Q6	.224	198	.000	.855	198	.000
Q7	.228	198	.000	.882	198	.000
Q9	.205	198	.000	.901	198	.000

a. Lilliefors Significance Correction

11-5-3 التحقق من عدم وجود فروق بين احكام المجموعتين التجريبيتين نتيجة عوامل أخرى بخلاف بديل الإفصاح عن إدارة المخاطر السيبرانية:

تم اختبار الفرق بين أحكام المجموعتين فيما يتعلق بتقديراتهم لأسعار الأسهم وقرارهم بشأن الاستثمار في الأسهم (كمستثمرين) والتعامل على الخدمات الالكترونية للبنك (كعملاء) قبل الحصول على الإفصاح الخاص بإدارة المخاطر السيبرانية، وذلك باستخدام اختبار مان ويتني للفرق بين المجموعتين المستقلتين.

جدول 9: اختبار مان ويتني لاختبار عدم وجود فروق معنوية بين أحكام مجموعتي التجربة قبل الحصول على بديلي الإفصاح عن إدارة المخاطر السيبرانية **(على مستوى المهنيين)**				
الاختبار الاحصائي	**الاختبار المستخدم**	**N**	**Z**	**P-value**
معنوية الفرق بين تقييم المشاركين في المجموعتين التجريبيتين الدراسة لأسعار الأسهم قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q2)**	Mann-Whitney	المجموعة الأولى 62 مشاهدة المجموعة الثانية 53 مشاهدة	1.566	.117
معنوية الفرق بين قرار المشاركين في المجموعتين التجريبيتين للاستثمار في أسهم البنك قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q3)**			.970	.332
معنوية الفرق بين قرار المشاركين في المجموعتين التجريبيتين لاستخدام الخدمات الالكترونية وبطاقات ائتمان البنك قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q4)**			.332	.740

وجاءت النتائج (س2، س3، س4) لتشير بعدم وجود فروق معنوية بين أحكام المجموعة الأولى (التي تتلقى لاحقاً الإفصاح من خلال تقرير مجلس الإدارة) أو المجموعة الثانية التي تتلقى لاحقاً الإفصاح ضمن تقرير مستقل (جدول رقم 9).

كما تم تطبيق الاختبار أيضاً على مستوى الأكديميين وتوصلت النتائج لعدم وجود فروق معنوية بين أحكام المجموعتين التجريبيتين من الأكاديميين قبل حصولهم على بديلي الإفصاح (جدول رقم 10)

جدول 10: اختبار مان ويتني لاختبار عدم وجود فروق معنوية بين أحكام مجموعتي التجربة قبل الحصول على بديلي الإفصاح عن إدارة المخاطر السيبرانية **(على مستوى الاكاديميين)**				
الاختبار الاحصائي	**الاختبار المستخدم**	**N**	**Z**	**P-value**
معنوية الفرق بين تقييم المشاركين في المجموعتين التجريبيتين الدراسة لأسعار الأسهم قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q2)**	Mann-Whitney	المجموعة الأولى 40 مشاهدة المجموعة الثانية 43 مشاهدة	1.409	.159
معنوية الفرق بين قرار المشاركين في المجموعتين التجريبيتين للاستثمار في أسهم البنك قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q3)**			1.056	.291
معنوية الفرق بين قرار المشاركين في المجموعتين التجريبيتين لاستخدام الخدمات الالكترونية وبطاقات ائتمان البنك قبل الحصول إفصاح إدارة مخاطر الأمن السيبراني **(Q4)**			.563	.573

وتشير النتائج السابقة إلى أن أي اختلاف قد ينتج بين أحكام المستخدمين في المرحلة التالية للتجربة سيكون راجعاً بصورة أساسية إلى اختلاف بديلي الإحصاء بما يقدم دعماً للنتائج وتأكيداً على تحييد العوامل الأخرى.

6-11 <u>اختبارات الفروض:</u>

اعتمد الباحث في اختبارات الفروض على الاختبارات اللامعلمية، نظراً لطبيعة البيانات والتي لا تتبع التوزيع الطبيعي. وتم اختبار فروض الدراسة بصفة أساسية بالتطبيق على **المحللين الماليين ومديري الاستثمار**، وكاختبارات تحليل الحساسية سيتم إعادة اختبار الفروض تطبيقاً على **أعضاء هيئة التدرس** للحصول على فهما أكبر للفرق بين الأكاديميين والمهنيين في هذا السياق.

11-6-1اختبار الفرض الأول:

تم استخدام اختبار Wilcoxon لاختبار الفرق بين أحكام المشاركين وذلك من خلال التطبيق على كل مجموعة على حده، حيث:

- تم مقارنة الفرق بين أحكام المشاركين (**المهنيين**) في ظل عدم الإفصاح عن إدارة المخاطر السيبرانية مقابل الإفصاح عنها ضمن تقرير مجلس الإدارة بالنسبة للمجموعة الأولى.
- تم مقارنة الفرق بين أحكام المشاركين (**المهنيين**) في ظل عدم الإفصاح عن إدارة المخاطر السيبرانية مقابل الإفصاح عنها ضمن تقرير منفصل بالنسبة للمجموعة الثانية.

ويمكن صياغة هذا الفرض إحصائياً على النحو التالي:

- **فرض العدم (H_0):** M1=M2 ويعني عدم وجود فرق معنوي بين أحكام المجموعة التجريبية قبل الحصول على الإفصاح عن إدارة المخاطر البيئية مقارنة بأحكامهم بعد الحصول على الإفصاح (لكل بديل من بديلي الإفصاح)
- **الفرض البديل (H1): M1 ≠ M2** ويعني وجود فرق معنوي بين أحكام المجموعة التجريبية قبل الحصول على الإفصاح عن إدارة المخاطر البيئية مقارنة بأحكامهم بعد الحصول على الإفصاح (لكل بديل من بديلي الإفصاح)

وأيدت النتائج وجود فرق معنوي بين أحكام المستخدمين بعد حصولهم على الإفصاح عن إدارة مخاطر الأمن السيبرني في كل من بديلي الإفصاح. **ويشير ذلك إلى قبول فرض الدراسة الأول** عند مستوى معنوية 5% لكل مجموعة من المجموعتين التجريبيتين (جدولي نتائج 11 و 12). حيث كان هناك أثر معنوي للإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة على أحكام المستثمرين بشأن تقييم أسهم البنك (P-value= .014)، وقرار الاستثمار في أسهم البنك (p-value= .000)، وعلى رغبة العملاء في التعامل على خدمات البنك الالكترونية واستخدام البطاقات الائتمانية لاتمام التعاملات الالكترونية (P-value= .000)، بما يشير إلى رفض فرض العدم وقبول الفرض البديل لفرض الدراسة الفرعي الأول من الفرض الأول (H1-a).

كما كان هناك أثر معنوي للإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل على أحكام المستثمرين بشأن تقييم أسهم البنك (P-value= .000)، وقرار الاستثمار في أسهم البنك (p-value= .000)، ورغبة العملاء في التعامل على خدمات البنك الالكترونية واستخدام البطاقات الائتمانية لاتمام التعاملات الالكترونية (P-value= .034)، بما يشير إلى رفض فرض العدم وقبول الفرض البديل لفرض الدراسة الفرعي الثاني من الفرض الأول (H1-b).

جدول 11: Wilcoxon Signed Ranks Test
على مستوى المهنيين

		Q6-Q2			Q7-Q3			Q9-Q4		
		N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks
المجموعة الأولى (الإفصاح ضمن تقرير مجلس الإدارة)	Negative Ranks	9[a]	17.28	155.50	2[d]	17.00	34.00	6[g]	30.17	181.00
	Positive Ranks	24[b]	16.90	405.50	32[e]	17.53	561.00	54[h]	30.54	1649.00
	Ties	29[c]			28[f]			2[i]		
	Total	62			62			62		
المجموعة الثانية (الإفصاح ضمن تقرير منفصل)	Negative Ranks	7[a]	18.29	128.00	1[d]	9.00	9.00	9[g]	13.50	121.50
	Positive Ranks	37[b]	23.30	862.00	36[e]	19.28	694.00	20[h]	15.68	313.50
	Ties	9[c]			16[f]			24[i]		
	Total	53			53			53		
		a. Q6 < Q2 b. Q6 > Q2 c. Q6 = Q2			d. Q7 < Q3 e. Q7 > Q3 f. Q7 = Q3			g. Q9 < Q4 h. Q9 > Q4 i. Q9 = Q4		

جدول 12: نتائج اختبار ويلكوكسن لاختبار فرض الدراسة الأول
بالتطبيق على المهنيين

	الفرض	القرار	الاختبار الاحصائي	اسم الاختبار	Z	P-value
H1a	يؤثر إفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة معنوياً على أحكام عملائها والمستثمرين في أسهمها	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم المشاركين لأسعار الأسهم قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني	Wilcoxon Test	2.466	.014
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين قرار المشاركين لشراء السهم قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني		5.096	.000
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك **Q4 v.s Q9**	معنوية الفرق بين قرار العملاء للتعامل في الخدمات الالكترونية للبنك واستخدام البطاقات الائتمانية قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني		5.517	.000
H1b	يؤثر إفصاح البنوك في مصر عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل معنوياً على أحكام عملائها والمستثمرين في أسهمها	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم المشاركين لأسعار الأسهم قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني	Wilcoxon Test	4.488	.000
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين قرار المشاركين لشراء السهم قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني		5.304	.000
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك **Q4 v.s Q9**	معنوية الفرق بين قرار العملاء للتعامل في الخدمات الالكترونية للبنك واستخدام البطاقات الائتمانية قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني		2.122	.034

ويبقى تساؤل حول أي من بديلي الإفصاح له تأثير أكثر معنوية على أحكام المستفيدين، وهو ما يتم اختبار من خلال الفرض الفرعي الثالث لفرض الدراسة الأول (H1-c)، وباستخدام اختبار Mann-Whitney Test للعينات المستقلة جاءت النتائج لتشير إلى أن الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل

له أثر أكثر معنوية على تقييم المستثمرين لأسعار الأسهم (Q6)، وقرار الاستثمار في أسهم البنك (Q7)، بينما لم يكن هناك تأثير معنوي لبديلي الإفصاح في الأثر على قرار العملاء لاستخدام الخدمات الالكترونية وبطاقات الائتمان للبنك (Q9) (جدول رقم 13)، وبالتالي يمكن القول برفض فرض العدم لهذا الفرض الفرعي وقبول الفرض البديل فقط فيما يتعلق بقرارات الاستثمار وليس قرارات العملاء للتعامل مع الخدمات الالكترونية للبنك.

جدول 13: Mann-Whitney Test
بالتطبيق على المهنيين
Ranks Test Statistics

	Group	N	Mean Rank	Sum of Ranks	z	p-value
Q6	Group (1)	62	51.40	3187.00		
	Group (2)	53	65.72	3483.00	2.448	.014
	Total	115				
Q7	Group (1)	62	52.31	3243.00		
	Group (2)	53	64.66	3427.00	2.074	.038
	Total	115				
Q9	Group (1)	62	58.81	3646.00		
	Group (2)	53	57.06	3024.00	.285	.776
	Total	115				

اختبار إضافي: (اختبار معنوية اعتماد على الإفصاح المقدم لاتخاذ القرار المطلوب)

تم عمل اختبار إضافي للسؤال رقم (5) والخاص بما إذا كان الإفصاح المقدم بشأن إدارة الأمن السيبراني، يمكن الاعتماد عليه كأحد مدخلات قرار الاستثمار)، والسؤال رقم (8) والخاص بما إذا كان الإفصاح المقدم بشأن إدارة الأمن السيبراني، يمكن الاعتماد عليه كأحد مدخلات قرار التعامل على الخدمات الالكترونية للبنك، وقد جاءت جميع النتائج معنوية بما يشير إلى أن الإفصاح في كلاً من بديلي الإفصاح يقدم محتوى معلوماتي لكل من المستثمرين والعملاء وهو ما يدعم نتائج اختبار الفرضين الفرعيين (H1a) و (H1b) (جدول رقم 14). كما تم اختبار معنوية الفرق بين كل من بديلي الإفصاح وجاءت النتيجة معنوية في صالح الإفصاح من خلال التقرير المنفصل فيما يتعلق بالسؤال رقم (5) الخاص بقرار الاستثمار، وجاءت النتيجة غير معنوية بالنسبة للسؤال رقم (8) الخاص بقرار التعامل عبر الخدمات الالكترونية، وهو ما يدعم نتائج الاختبار الأساسي للفرض الفرعي (H1c) (جدول رقم 15).

جدول 14: اختبار معنوية اعتماد على الإفصاح المقدم لاتخاذ القرار المطلوب
One-Sample Test

Group		Test Value = 6					
		t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
						Lower	Upper
1	Q5	3.440	61	.001	.935	.39	1.48
	Q8	4.930	61	.000	1.194	.71	1.68
2	Q5	9.697	52	.000	2.283	1.81	2.76
	Q8	4.701	52	.000	1.358	.78	1.94

جدول 15: Mann-Whitney Test

على مستوى المهنيين

Ranks					Test Statistics	
	GROUP	N	Mean Rank	Sum of Ranks	z	p-value
Q5	1	62	48.11	2983.00	3.513	.000
	2	53	69.57	3687.00		
	Total	115				
Q8 d	1	62	54.44	3375.50	1.252	.211
	2	53	62.16	3294.50		
	Total	115				

11-6-2 اختبار الفرض الثاني:

يتسهدف هذا الفرض اختبار الأثر المعدل للجنس على العلاقة بين بدائل الإفصاح عن إدارة المخاطر السيبرانية وأحكام المستثمرين والعملاء بالبنوك. ويختبر فرض العدم لهذا الاختبار ما يلي:

- **فرض العدم** (H0): لا يختلف التأثير المعنوي لبديلي إفصاح البنوك المصرية عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس
- **الفرض البديل** (H1): يختلف التأثير المعنوي لبديلي إفصاح البنوك المصرية عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس

ولاختبار ذلك الفرض تم تقسميه إلى ثلاث فروض فرعية؛ الأول يتعلق ببديل الإفصاح من خلال تقرير مجلس الإدارة (H2-a)، والثاني يتعلق بالإفصاح في تقرير منفصل(H2-b)، والثالث يتعلق بالفرق بين بديلي الإفصاح (H2-c).

جدول 16: Wilcoxon Signed Ranks Test

على مستوى المهنيين

	الفرض	**القرار**	**الاختبار الاحصائي**	**N**	**Z**	**P-value**
H2a	يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير مجلس الإدارة على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	37	3.266	.001
			معنوية الفرق بين تقييم **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	25	.258	.799
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين قرار **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	37	4.600	.000
			معنوية الفرق بين تقييم **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	25	1.764	.078
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك واستخدام البطاقات الائتمانية **Q4 v.s Q9**	معنوية الفرق بين قرار **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	37	4.932	.000
			معنوية الفرق بين قرار **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	25	2.122	.034

وتشير النتائج بالجدول رقم (16) إلى أن تأثير الإفصاح عبر تقرير مجلس الإدارة عن مخاطر الأمن السيبراني للذكور كان معنوياً على تقييمهم لسعر السهم وقرار الاستثمار، وكذلك قرارا التعامل في الخدمات

الالكترونية للبنك، أما على مستوى النساء فلم يكن هناك تأثير على تقييمهن لأسعار الأسهم أو قرار الاستثمار في الأسهم وكان التأثير معنوياً على مستوى قرار التعامل في الخدمات الالكترونية للبنك. ويمكن ملاحظة أن قيمة (Z) المحسوبة على مستوى الذكور كانت أكبر من قيمتها لدى الإناث على مستوى كل القرارات، وبالتالي يمكن القول أن أحكام الذكور تتأثر معنوياً بصورة أكبر من الإناث بالحصول على إفصاحات عن إدارة مخاطر الأمن السيبراني عبر تقرير مجلس الإدارة.

اختبار إضافي: (معنوية الفرق بين قرارات الذكور والإناث بعد حصولهم على الإفصاح للمجموعة التجريبية الأولى)

للوقوف على معنوية الفرق بين قرارات الذكور والإناث بعد حصولهم على الإفصاح عن إدارة مخاطر الأمن السيبراني، تم إجراء اختبار مان ويتني للعينات المستقلة بالتركيز على أحكام المشاركين بعد الحصول على ذلك الإفصاح من خلال تقرير مجلس الإدارة (الأسئلة س6، س 7، س9). وقد جاءت النتائج لتشير أن هناك فرق معنوي بين أحكام الجنسين، حيث تشير متوسطات الرتب إلى أن الذكور أعطوا تقييما أكبر للأسهم، وكانوا أكثر استعداداً للاستثمار في السهم، وللتعامل مع الخدمات الالكترونية للبنك مقارنة بالاناث، وكان ذلك معنوياً على مستوى قرارات المستثمرين سواء تقييم السهم (P-value= .010) أو الاستثمار في السهم (p-value- .031) غير أنه لم يكن معنوياً على مستوى قرارات العملاء بشأن التعامل على الخدمات الالكترونية للبنك عند مستوى معنوية 5% حيث جاءت (P-value= .074) (جدول رقم 17).

جدول 17: Mann-Whitney Test
على مستوى المهنيين

			Ranks		Test Statistics	
	GENDER	N	Mean Rank	Sum of Ranks	z	p-value
Q6	F	25	24.88	622.00		
	M	37	35.97	1331.00	2.561	.010
	Total	62				
Q7	F	25	25.72	643.00		
	M	37	35.41	1310.00	2.154	.031
	Total	62				
Q9	F	25	26.66	666.50		
d	M	37	34.77	1286.50	1.785	.074
	Total	62				

ولاختبار ذلك فيما يتعلق بالإفصاح من خلال تقرير منفصل (H2-b) ، تم إعادة الاختبار على المجموعة التجريبية الثانية، وجاءت النتائج كما بالجدول رقم (18). والتي تشير إلى أن تأثير الإفصاح عبر تقرير منفصل عن مخاطر إدارة الأمن السيبراني للذكور والإناث كان معنوياً على تقييمهم لسعر السهم وقرار الاستثمار، وقرار التعامل في الخدمات الالكترونية للبنك. كما يمكن ملاحظة أن قيمة (Z) المحسوبة على مستوى الذكور كانت أكبر من قيمتها لدى الإناث، وبالتالي يمكن القول أن أحكام الذكور تتأثر بصورة أكبر من الإناث بالحصول على إفصاحات عن إدارة مخاطر الأمن السيبراني عبر تقرير منفصل.

جدول 18: Wilcoxon Signed Ranks Test
على مستوى المهنيين

الفرض		القرار	الاختبار الاحصائي	N	Z	P-value
H2b	يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير منفصل على أحكام عملائها والمستثمرين في أسهمها باختلاف الجنس	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	31	3.646	.000
			معنوية الفرق بين تقييم **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	22	2.627	.009
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين قرار **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	31	4.118	.000
			معنوية الفرق بين تقييم **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	22	3.390	.001
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك **Q4 v.s Q9**	معنوية الفرق بين قرار **الذكور** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	31	3.108	.002
			معنوية الفرق بين قرار **الإناث** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن منفصل	22	2.031	.042

<u>اختبار إضافي:</u> (معنوية الفرق بين قرارات الذكور والإناث بعد حصولهم على الإفصاح للمجموعة التجريبية الثانية)

للوقوف على معنوية الفرق بين قرارات الذكور والإناث بع حصولهم على الإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل، تم إجراء اختبار مان ويتني للعينات المستقلة بالتركيز على أحكام المشاركين بعد الحصول على ذلك الإفصاح (من خلال الأسئلة س6، س 7، س9). وقد جاءت النتائج بجدول رقم (19) لتشير أن هناك فرق معنوي بين أحكام الجنسين فقط فيما يتعلق بقرار التعامل مع الخدمات الالكترونية للبنك.

جدول 19: Mann-Whitney Test
على مستوى المهنيين

			Ranks		Test Statistics	
	GENDER	N	Mean Rank	Sum of Ranks	z	p-value
Q6	F	22	28.36	624.00		
	M	31	26.03	807.00	.583	.560
	Total	53				
Q7	F	22	26.61	585.50		
	M	31	27.27	845.50	.163	.871
	Total	53				
Q9	F	22	19.93	438.50		
d	M	31	32.02	992.50	.871	.005
	Total	53				

ولغرض اختبار الفرق بين قرارات الذكور والإناث بعد الحصول على الافصاح ضمن تقرير مجلس الادارة مقارنة بالافصاح في تقرير مستقل (H2-c) تم استخدام اختبار Mann-Whitney Test للعينات المستقلة حيث تم اختبار الفرق بين أحكام الذكور في ظل بديلي الإفصاح، وكذلك أحكام الإناث في ظل بديلي الإفصاح. وجاءت النتائج كما بجدول رقم (20).

ففي حين أشارت نتائج اختبار الفرض الفرعي (H1-c) أن هناك فرق معنوي بين قرارات المشاركين باختلاف بديل الإفصاح وذلك فيما يتعلق بالقرارات التي تخص المستثمرين وليس قرارات العملاء فيما يتعلق بالتعامل على

الخدمات الالكترونية للبنك، إلا أن نتائج اختبار الفرض (H2-c) بجدول رقم (20) أشارت إلى أن تلك النتيجة تختلف باختلاف الجنس، حيث تتحقق تلك النتيجة على مستوى الإناث دون الذكور. وبالتالي يمكن القول أن الجنس يؤثر في العلاقة بين بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني وأحكام المستثمرين. إلا أن الجنس لم يكن له تأثير على مستوى أحكام عملاء البنك فيما يتعلق بقرار التعامل على الخدمات الالكترونية للبنك.

جدول 20: Mann-Whitney Test

على مستوى المهنيين

Ranks **Test Statistics**

GENDER	Group		N	Mean Rank	Sum of Ranks	z	p-value
F	Q6	1	25	18.18	454.50		
		2	22	30.61	673.50	3.338	.001
		Total	47				
	Q7	1	25	19.62	490.50		
		2	22	28.98	637.50	2.443	.015
		Total	47				
	Q9	1	25	26.62	665.50		
		2	22	21.02	462.50	1.431	.152
		Total	47				
M	Q6	1	37	33.45	1237.50		
		2	31	35.76	1108.50	.512	.609
		Total	68				
	Q7	1	37	33.31	1232.50		
		2	31	35.92	1113.50	.570	.569
		Total	68				
	Q9	1	37	32.65	1208.00		
		2	31	36.71	1138.00	.859	.390
		Total	68				

11-6-3 اختبار الفرض الثالث:

يتسهدف هذا الفرض اختبار الأثر المعدل للعمر على العلاقة بين بدائل إفصاح البنوك عن إدارة المخاطر السيبرانية وأحكام المستثمرين والعملاء. ويختبر فرض العدم لهذا الاختبار ما يلي:

- **فرض العدم** (H0): لا يختلف التأثير المعنوي لبديلي إفصاح البنوك المصرية عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف العمر
- **الفرض البديل** (H1): يختلف التأثير المعنوي لبديلي إفصاح البنوك المصرية عن إدارة المخاطر السيبرانية على أحكام عملائها والمستثمرين في أسهمها باختلاف العمر

ولاختبار ذلك الفرض تم تقسيمه إلى ثلاث فروض فرعية الأول يتعلق ببديل الإفصاح من خلال تقرير مجلس الإدارة (H3-a) الثاني يتعلق بالإفصاح في تقرير منفص (H3-b)، والثالث يتعلق بالفرق بين بديلي الإفصاح (H3-c).

جدول 21: Wilcoxon Signed Ranks Test - على مستوى المهنيين						
	الفرض	القرار	الاختبار الاحصائي	N	Z	P-value
H3a	يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير مجلس الإدارة على أحكام عملائها والمستثمرين في أسهمها **باختلاف العمر**	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	26	1.508	.132
			معنوية الفرق بين تقييم **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	36	4.212	.000
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين قرار **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	26	1.518	.129
			معنوية الفرق بين تقييم **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	36	5.064	.000
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك واستخدام البطاقات الائتمانية **Q4 v.s Q9**	معنوية الفرق بين قرار **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	26	1.764	.078
			معنوية الفرق بين قرار **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير مجلس الإدارة	36	2.309	.021

وتشير النتائج بالجدول رقم (21) إلى أن تأثير الإفصاح **عبر تقرير مجلس الإدارة** عن مخاطر الأمن السيبراني لكبار السن كان معنوياً على تقييمهم لسعر السهم وقرار الاستثمار (كمستثمرين) وقرار التعامل في الخدمات الالكترونية. أما بالنسبة لصغار السن فلم يكن للإفصاح عبر تقرير مجلس الإدارة أي تأثير معنوي لأي من القرارات، وبالتالي يمكن القول أن عامل السن يعدل من العلاقة بين الإفصاح من خلال بديل تقرير مجلس الإدارة وأحكام المستخدمين فيما يتعلق بقرارات الاستثمار.

<u>اختبار إضافي:</u>(معنوية الفرق بين قرارات الأكبر والأصغر سناً بعد حصولهم على الإفصاح للمجموعة التجريبية الأولى)

للوقوف على معنوية الفرق بين قرارات الأكبر سناً والأصغر سناً بعد حصولهم على الإفصاح عن إدارة مخاطر الأمن السيبراني، تم إجراء اختبار مان ويتني للعينات المستقلة بالتركيز على أحكام المشاركين بعد الحصول على ذلك الإفصاح (من خلال الأسئلة س6، س 7، س9). وقد جاءت النتائج بجدول (22) لتشير لوجود فرق معنوي بين أحكام الفئتين العمريتين عند مستوى معنوية 5%، فيما يتعلق بقرارات الاستثمار فقط، وبالتالي يمكن القول أن عامل العمر له تأثير معدل جزئياً على العلاقة بين الإفصاح من خلال تقرير مجلس الإدارة وأحكام المستخدمين.

جدول 22: Mann-Whitney Test - على مستوى المهنيين						
		Ranks			Test Statistics	
	AGE	N	Mean Rank	Sum of Ranks	z	p-value
Q6	OLD	36	37.31	1343.00	3.235	.001
	YOUNG	26	23.46	610.00		
	Total	62				
Q7	OLD	36	36.50	1314.00	2.720	.007
	YOUNG	26	24.58	639.00		
	Total	62				
Q9	OLD	36	28.17	1014.00	1.760	.078
	d YOUNG	26	36.12	939.00		
	Total	62				

ولاختبار ذلك فيما يتعلق بالإفصاح من خلال تقرير منفصل (H3–b) ، تم إعادة الاختبار على المجموعة التجريبية الثانية، وجاءت النتائج كما بالجدول رقم (23). وتشير النتائج بالجدول رقم (23) إلى أن تأثير الإفصاح عبر تقرير منفصل عن مخاطر الأمن السيبراني لكل من الأكبر عمراً والأصغر عمراً كان معنوياً على تقييمهم لسعر السهم وقرار الاستثمار، وكذلك قرارا التعامل في الخدمات الالكترونية للبنك. ويمكن ملاحظة أن قيمة (Z) المحسوبة على مستوى الأكبر سناً كانت أكبر من قيمتها لدى الأصغر سناً على مستوى كل القرارات ما عدا قرار التعامل مع الخدمات الالكترونية للبنك.

جدول 23: Wilcoxon Signed Ranks Test- **على مستوى المهنيين**

الفرض		القرار	الاختبار الاحصائي	N	Z	P-value
H3b	يختلف التأثير المعنوي لإفصاح البنوك في مصر عن إدارة المخاطر السيبرانية من خلال تقرير منفصل على أحكام عملائها والمستثمرين في أسهمها **باختلاف العمر**	تقييم المستثمرين لسعر السهم **Q2 v.s Q6**	معنوية الفرق بين تقييم **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	37	2.683	.007
			معنوية الفرق بين تقييم **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	16	2.899	.004
		قرار المستثمرين للاستثمار في السهم **Q3 v.s Q7**	معنوية الفرق بين تقييم **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	37	2.840	.005
			معنوية الفرق بين قرار **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	16	4.264	.000
		قرار العملاء للتعامل في الخدمات الالكترونية للبنك واستخدام البطاقات الائتمانية **Q4 v.s Q9**	معنوية الفرق بين قرار **للأصغر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	37	4.369	.000
			معنوية الفرق بين قرار **للأكبر عمراً** قبل وبعد الحصول على الإفصاح عن إدارة الأمن السيبراني ضمن تقرير منفصل	16	3.458	.001

<u>اختبار إضافي:</u>(معنوية الفرق بين قرارات الأكبر والأصغر سناً بعد حصولهم على الإفصاح للمجموعة التجريبية الثانية)

للوقوف على معنوية الفرق بين قرارات الفئتين العمريتين بعد حصولهم على الإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير منفصل، تم إجراء اختبار مان ويتني للعينات المستقلة بالتركيز على أحكام المشاركين بعد الحصول على ذلك الإفصاح (من خلال الأسئلة س6، س 7، س9). وقد جاءت النتائج بجدول رقم (24) لتشير لعدم وجود فرق معنوي بين أحكام الفئتين، إلا فيما يخص قرار الاستثمار حيث كان أثر الإفصاح على قرارات صغار السن أكثر معنوية مقارنة بكبار السن. وبالتالي يمكن القول بأن عامل العمر كان له تأثيراً جزئياً على العلاقة بين الإفصاح **من خلال تقرير منفصل** وبين أحكام المتعاملين، فضلاً عن أن هذا التقرير له محتوى معلوماتي لكل من صغار السن وكبار السن في جميع القرارات.

جدول 24: Mann-Whitney Test- **على مستوى المهنيين**

			Ranks		Test Statistics	
	AGE	N	Mean Rank	Sum of Ranks	z	p-value
Q6	YOUNG	37	25.34	937.50		
	OLD	16	30.84	493.50	1.284	.199
	Total	53				
Q7	YOUNG	37	30.81	1140.00		
	OLD	16	18.19	291.00	2.899	.004
	Total	53				
Q9	YOUNG	37	28.78	1065.00		
d	OLD	16	22.88	366.00	1.292	.197
	Total	53				

ولغرض اختبار الفرق بين قرارات الأكبر سناً والأقل سناً بعد الحصول على الافصاح ضمن تقرير مجلس الادارة مقارنة بالافصاح في تقرير مستقل (H3-c) تم استخدام اختبار Mann-Whitney Test للعينات المستقلة حيث تم اختبار الفرق بين أحكام الأكبر سناً في ظل بديلي الإفصاح، وكذلك أحكام الأصغر سناً في ظل بديلي الإفصاح، وجاءت النتائج على النحو التالي جدول رقم (25):

جدول 25: Mann-Whitney Test - **على مستوى المهنيين**

			Ranks		Test Statistics		
AGE	Group		N	Mean Rank	Sum of Ranks	z	p-value
YOUNG	Q6	1	26	27.42	713.00		
		2	37	35.22	1303.00	2.899	.004
		Total	63				
	Q7	1	26	23.71	616.50		
		2	37	37.82	1399.50	3.162	.002
		Total	63				
	Q9	1	26	32.38	842.00		
		2	37	31.73	1174.00	.142	.887
		Total	63				
OLD	Q6	1	36	23.68	852.50		
		2	16	32.84	525.50	2.148	.032
		Total	52				
	Q7	1	36	27.71	997.50		
		2	16	23.78	380.50	.902	.376
		Total	52				
	Q9	1	36	27.44	988.00		
		2	16	24.38	390.00	.693	.448
		Total	52				

ففي حين أشارت نتائج اختبار الفرض الفرعي (H1–c) إلى أن هناك فرق معنوي بين قرارات المشاركين باختلاف بديل الإفصاح وذلك فيما يتعلق بالقرارات التي تخص المستثمرين وليس قرارات العملاء الخاصة بالتعامل على الخدمات الالكترونية للبنك، إلا أن نتائج اختبار الفرض (H3–c) أشارت إلى أن تلك النتيجة تختلف باختلاف العمر، حيث تتحقق تلك النتيجة على مستوى الأصغر سناً فيما يتعلق بقرار تقييم الأسهم وقرار الاستثمار، وتتحقق بالنسبة لكبار السن فيما يتعلق بحكمهم في تقييم السهم. وبالتالي يمكن القول أن العمر يؤثر جزئياً على العلاقة

بين بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني وأحكام المستثمرين، إلا أن العمر لم يكن له تأثير على مستوى أحكام عملاء البنك فيما يتعلق بقرار التعامل على الخدمات الالكترونية للبنك.

اختبارات الحساسية: (إعادة اختبار الفروض على عينة من الأكاديميين)

لاختبار حساسية النتائج باختلاف فئة المشاركين، فقد تم إعادة تطبيق الاختبارات الأساسية السابقة على عينة من الأكاديميين للوقوف على الفرق في أحكام المهنيين والأكاديميين فيما يتعلق بأهمية الإفصاح عن إدارة مخاطر الأمن السيبراني وتأثير ذلك على القرارات.

وأشارت النتائج بجدول رقم (26) إلى الآتي: بالنسبة للمجموعة التجريبية الأولى التي تلقت الإفصاح ضمن تقرير مجلس الإدارة فلا يوجد تأثير معنوي للإفصاح عن إدارة مخاطر السيبرانية على أحكام المستخدمين كمستثمرين (تقييم الأسهم أو قرار الاستثمار)، وكان هناك تأثير معنوي على قراراتهم كعملاء (من خلال قرار التعامل على الخدمات الالكترونية للبنك). أما المجموعة التجريبية الثانية والتي تلقت الإفصاح من خلال تقرير منفصل عن إدارة مخاطر الأمن السيبرني فقد جاءت النتائج لتشير لوجود تأثير معنوي لذلك الإفصاح عل كافة قراراتهم سواء على مستوى قرارات المستثمرين (تقييم السهم، واتخاذ قرار الاستثمار)، أو قرارات العملاء (بالتعامل على الخدمات الالكترونية للبنك).

جدول 26: Wilcoxon Signed Ranks Test - **على مستوى الأكاديميين**

Test Statistics

Group		Q6 - Q2	Q7 - Q3	Q9 - Q4
1	Z	-1.129[a]	-.962[b]	-3.806[b]
	Asymp. Sig. (2-tailed)	.259	.336	.000
2	Z	-2.877[b]	-4.550[b]	-4.788[b]
	Asymp. Sig. (2-tailed)	.004	.000	.000

a. Based on positive ranks.
b. Based on negative ranks.

وبمقارنة أحكام المشاركين في المجموعة الأولى (الإفصاح من خلال تقرير مجلس الإدارة) مقابل المحموعة الثانية (الإفصاح من خلال تقرير منفصل)، أتضح وجود فرق معنوي فيما يتعلق بأحكام المشاركين كمستثمرين (تقييم الأسهم، وقرار الاستثمار)، إلى أنه لا يوجد فرق معنوي فيما يتعلق بقرار العملاء للتعامل عبر الخدمات الاكترونية للبنك (جدول نتائج رقم 27)، وهو ما يدعم النتيجة السابقة.

وبجمع تلك النتائج معاً يمكن القول بأن الإفصاح من خلال التقرير المنفصل له تأثير معنوي على قرارات وأحكام المشاريكين سواء كمستثمرين أو عملاء، بينما الإفصاح من خلال تقرير مجلس الإدارة يحسن فقط من قرارات العملاء وليس المستثمرين، وذلك على مستوى الأكاديميين.

جدول 27: Mann-Whitney Test - على مستوى الأكاديميين

Ranks **Test Statistics**

	Group	N	Mean Rank	Sum of Ranks	z	p-value
Q6	Group (1)	40	29.00	1160.00		
-	Group (2)	43	54.09	2326.00	4.963	.000
	Total	83				
Q7	Group (1)	40	28.80	1152.00		
	Group (2)	43	54.28	2334.00	5.047	.000
	Total	83				
Q9	Group (1)	40	42.45	1698.00		
	Group (2)	43	41.58	1788.00	.169	.866
	Total	83				

وباختبار **أثر الجنس** على علاقة الإفصاح عن إدارة الأمن السيبراني وأحكام المشاركين، فقد جاءت النتائج على مستوى المجموعة الأولى (الإفصاح من خلال تقرير مجلس الإدارة) لتشير إلى أن ذلك الإفصاح يؤدي إلى تحسن قرارات العملاء (التعامل على الخدمات الالكترونية للبنك) دون أن يؤثر معنوياً على قرارات تقييم الأسهم والاستثمار، وذلك على مستوى الذكور (M) والإناث (F) للأكاديميين، بما يعني عدم وجود أثر معنوي للجنس في هذا الإطار(جدول نتائج رقم 28).

جدول 28: Wilcoxon Signed Ranks Test - **على مستوى الأكاديميين**

Test Statistics

GENDER		Q6 - Q2	Q7 - Q3	Q9 - Q4
F	Z	1.498[a]	1.414[b]	2.558[b]
	Asymp. Sig. (2-tailed)	.134	.157	.011
M	Z	.378[b]	.333[a]	2.972[b]
	Asymp. Sig. (2-tailed)	.705	.739	.003

a. Based on positive ranks.
b. Based on negative ranks.

أما على مستوى المجموعة التجريبية الثانية والمتعلقة بالحصول على الإفصاح من خلال تقرير منفصل عن إدارة مخاطر الأمن السيبراني فقد جاءت النتائج تشير إلى وجود أثر معنوي على أحكام كل من الذكور والإناث سواء تقييم الأسهم أو الاستثمار أو التعامل في الخدمات الالكترونية (جدول رقم 29).

جدول 29: Wilcoxon Signed Ranks Test - **على مستوى الأكاديميين**

Test Statistics

GENDER		Q6 - Q2	Q7 - Q3	Q9 - Q4
F	Z	2.230[a]	2.887[a]	3.318[a]
	Asymp. Sig. (2-tailed)	.026	.004	.001
M	Z	2.076[a]	3.493[a]	3.502[a]
	Asymp. Sig. (2-tailed)	.038	.000	.000

a. Based on positive ranks.
b. Based on negative ranks.

وللوقوف على ما إذا كان هناك فرقاً معنوياً بين أحكام الذكور والإناث تم اجراء اختبار Mann–Whitney Test للعينات المستقلة، وأشارت النتائج لعدم وجود فرق معنوي بين أحكام الذكور أو الإناث سواء قبل الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني أو بعد الحصول على الإفصاح عن مخاطر الأمن السيبراني. بما

يشير إلى أن الجنس ليس له تأثير معنوي على العلاقة بن بديلي الإفصاح عن مخاطر الأمن السيبراني وبين أحكام المشاركين (جدول رقم 30)

جدول 30: Mann-Whitney Test - **على مستوى الأكاديميين**
Test Statistics (F) v.s (M)

Group		Q2	Q3	Q4	Q6	Q7	Q9
Group(1)	Z	.733	.301	.058	.782	.657	1.341
	Asymp. Sig. (2-tailed)	.464	.764	.954	.434	.511	.180
Group(1)	Z	1.256	.701	1.086	1.250	.446	1.065
	Asymp. Sig. (2-tailed)	.209	.483	.278	.211	.655	.287

وباختبار أثر **العمر** على علاقة الإفصاح عن إدارة الأمن السيبراني وأحكام المشاركين، فقد كانت النتائج على مستوى المجموعة الأولى (الإفصاح من خلال تقرير مجلس الإدارة) تشير إلى أن ذلك الإفصاح يؤدي إلى تحسن قرارات العملاء (التعامل على الخدمات الالكترونية للبنك) دون أن يؤثر معنوياً على قرارات تقييم الأسهم والاستثمار، وذلك على مستوى الأكبر سناً والأصغر سناً للأكاديميين (جدول نتائج رقم 31).

جدول 31: Wilcoxon Signed Ranks Test - **على مستوى الأكاديميين**
Test Statistics

AGE		Q6 - Q2	Q7 - Q3	Q9 - Q4
YOUNG	Z	.577[a]	.577[a]	3.369[a]
	Asymp. Sig. (2-tailed)	.564	.564	.001
OLD	Z	1.890[b]	.775[a]	2.237[a]
	Asymp. Sig. (2-tailed)	.059	.439	.025

a. Based on positive ranks.
b. Based on negative ranks.

أما على مستوى المجموعة التجريبية الثانية والمتعلقة بالحصول على الإفصاح من خلال تقرير منفصل عن إدارة مخاطر الأمن السيبراني فقد جاءت النتائج تشير إلى وجود أثر معنوي على أحكام الأكبر سناً والأصغر سناً فيما يتعلق بقرارات العملاء بالتعامل في الخدمات الالكترونية، أما فيما يتعلق بقرارات تقييم الأسهم والاستثمار فقط كانت الإفصاح ضمن تقرير منفصل له أثر معنوي على أحكام المستثمرين الأكبر سنا وليس الأصغر سناً (جدول رقم 32).

جدول 32: Wilcoxon Signed Ranks Test - **على مستوى الأكاديميين**
Test Statistics

AGE		Q6 - Q2	Q7 - Q3	Q9 - Q4
YOUNG	Z	.687[a]	1.785[a]	1.979[a]
	Asymp. Sig. (2-tailed)	.492	.074	.048
OLD	Z	2.900[a]	3.582[a]	4.153[a]
	Asymp. Sig. (2-tailed)	.004	.000	.000

a. Based on positive ranks.
b. Based on negative ranks.

وللوقوف على ما إذا كان هناك فرقاً معنوياً بين أحكام الأكبر سناً ووالأصغر سناً تم اجراء اختبار Mann–Whitney Test للعينات المستقلة، وأشارت النتائج (جدول رقم 33) إلى أنه على مستوى قرارات الاستثمار كان هناك فرقاً معنوياً في تقييم الأسهم بين الأكبر سنا والأصغر سناً قبل الحصول على الإفصاح في صالح المستثمرين الأصغر سناً، غير أن ذلك الفرق أصبح غير معنوي بعد الحصول على الإفصاح في بديلي الإفصاح. وعلى جانب أخر لم يكن هناك فرقاً معنوياً بين المستثمرين الأكبر سناً والأصغر سناً فيما يتعلق بقرار الاستثمار في الأسهم أو

قرار التعامل على الخدمات الالكترونية للبنك، إلا أن هذا الفرق أصبح معنوياً بين كبار الأكبر سناً والأصغر سناً لصالح الأكبر سناً في ظل البديل الثاني للإفصاح من خلال التقرير المستقل فقط.

وتشير تلك النتائج السابقة معاً إلى أن عامل العمر يعدل معنوياً من العلاقة بين بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات المشاركين الأكاديميين. وأن الأكبر سناً هم الأكثر استفادة من الإفصاح عن إدارة مخاطر الأمن السيبراني، وأنهم يأخذون تلك الإفصاحات بعين الاعتبار عند اتخاذ قراراتهم، لا سيما عند الحصول على ذلك الإفصاح في شكل تقرير منفصل.

جدول 33: Mann-Whitney Test - **على مستوى الأكاديميين**

Test Statistics (OLD) v.s (YOUNG)

Group		Q2	Q3	Q4	Q6	Q7	Q9
Group(1)	Z	2.252	1.084	1.348	.000	1.018	.284
	Asymp. Sig. (2-tailed)	.024	.279	.178	1.000	.309	.776
Group(2)	Z	3.721	1.521	.852	.719	2.900	2.634
	Asymp. Sig. (2-tailed)	.000	.128	.394	.472	.004	.008

جدول رقم (34)
ملخص نتائج أُثر بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني على أحكام المشاركين (ملخص نتائج فرض الدراسة الأول)

الاختبار الأساسي	فئة المهنيين								
	أحكام المستثمرين بخصوص تقييم السهم			أحكام المستثمرين بشأن قرار الاستثمار			أحكام العملاء بشأن التعامل في خدمات البنك الالكترونية		
	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة
الاختبارات الأساسية دون المتغيرات المعدلة	معنوي .014	معنوي .000	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة أو تقرير منفصل معنوياً على تقييم المستثمرين في سعر سهم البنك	معنوي .000	معنوي .000	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة أو تقرير منفصل معنوياً على قرار الاستثمار في سهم البنك	معنوي .000	معنوي .034	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة أو تقرير منفصل معنوياً على قرار عملاء البنك بالتعامل على خدماته الالكترونية
اختبار الفرق بين بديلي الإفصاح	معنوي .014		الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل له أثر أكثر معنوية على تقييم المستثمرين لأسعار الأسهم	معنوي .038		الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل له أثر أكثر معنوية على قرار الاستثمار في الأسهم	غير معنوي .776		لا يوجد فرق معنوي لبدائل الإفصاح عن إدارة مخاطر الأمن السيبراني على قرار عملاء البنك بالتعامل على خدماته الالكترونية
تحليل الحساسية	فئة الأكاديميين								
	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة	أثر الإفصاح من خلال تقرير مجلس الإدارة	أثر الإفصاح من خلال تقرير مستقل	تفسير النتيجة
الاختبارات الأساسية دون المتغيرات المعدلة	غير معنوي .259	معنوي .004	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني فقط من خلال تقرير منفصل معنوياً على تقييم المستثمرين في سعر سهم البنك	غير معنوي .336	معنوي .000	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني فقط من خلال تقرير منفصل معنوياً على قرار الاستثمار في سهم البنك	معنوي .000	معنوي .034	يؤثر الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير مجلس الإدارة أو تقرير منفصل معنوياً على قرار عملاء البنك بالتعامل على خدماته
اختبار الفرق بين بدسلي الإفصاح	معنوي .000		الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل له أثر أكثر معنوية على تقييم المستثمرين لأسعار الأسهم	معنوي .000		الإفصاح عن إدارة مخاطر الأمن السيبراني من خلال تقرير منفصل له أثر أكثر معنوية على قرار الاستثمار في الأسهم	غير معنوي .866		لا يوجد فرق معنوي لبدائل الإفصاح عن إدارة مخاطر الأمن السيبراني على قرار عملاء البنك بالتعامل على خدماته الالكترونية

جدول رقم (35)
ملخص نتائج **الأثر المعدل لجنس المشاركين** (ملخص نتائج **فرض الدراسة الثاني**)

(أ) الإفصاح من خلال تقرير مجلس الإدارة (H2a)

	أحكام المستثمرين بخصوص تقييم السهم		أحكام المستثمرين بشأن قرار الاستثمار		أحكام العملاء بشأن التعامل في خدمات البنك الالكترونية	
	الذكور	الإناث	تفسير النتيجة	الذكور	الإناث	تفسير النتيجة
أثر الإفصاح	معنوي .001	غير معنوي .799	كان تأثير الإفصاح على تقييم سعرالسهم معنوياً فقط على مستوى الذكور	معنوي .000	معنوي .078	كان تأثير الإفصاح على قرار الاستثمار معنوياً على مستوى الذكور فقط	معنوي .000	معنوي .034	كان تأثير الإفصاح على قرار التعامل على الخدمات الالكترونية معنوياً على مستوى الذكور والاناث
معنوية الفرق بين الذكور والاناث	معنوي .010		هناك فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير مجلس الإدارة	معنوي .031		هناك فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير مجلس الإدارة	غير معنوي .074		لا يوجد فرق معنوي بين قرارات الذكور أو الإناث للتعامل على الخدمات الالكترونية للبنك عند الحصول على الإفصاح من خلال تقرير مجلس الإدارة

(ب) الإفصاح من خلال تقرير منفصل (H2b)

	أحكام المستثمرين بخصوص **تقييم السهم**		أحكام المستثمرين بشأن **قرار الاستثمار**		أحكام العملاء بشأن **التعامل في خدمات البنك الالكترونية**	
	الذكور	الإناث	تفسير النتيجة	الذكور	الإناث	تفسير النتيجة
أثر الإفصاح	معنوي .000	معنوي .009	كان تأثير الإفصاح على تقييم سعرالسهم معنوياً على مستوى الذكور والإناث	معنوي .000	معنوي .001	كان تأثير الإفصاح على قرار الاستثمار معنوياً على مستوى الذكور والاناث	معنوي .002	غير معنوي .042	كان تأثير الإفصاح على قرار التعامل على الخدمات الالكترونية معنوياً على مستوى الذكور والاناث
معنوية الفرق بين الذكور والاناث	غير معنوي .560		لا يوجد فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير منفصل	غير معنوي .871		لا يوجد فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير منفصل	معنوي .005		يوجد فرق معنوي بين قرارات الذكور أو الإناث للتعامل على الخدمات الالكترونية للبنك عند الحصول على الإفصاح من خلال تقرير منفصل

(ج) الفرق بين معنوية أحكام المشاركين من خلال بديلي الإفصاح على مستوى كل من الذكور والإناث (H2c)

	أحكام المستثمرين بخصوص **تقييم السهم**		أحكام المستثمرين بشأن **قرار الاستثمار**		أحكام العملاء بشأن **التعامل في خدمات البنك الالكترونية**	
	P-value	تفسير النتيجة	P-value	تفسير النتيجة	P-value	تفسير النتيجة
الذكور	غير معنوي .609	لم يكن هناك فرق معنوي بين أحكام الذكور على مستوى بديلي الإفصاح	غير معنوي .569	لم يكن هناك فرق معنوي بين أحكام الذكور على مستوى بديلي الإفصاح	غير معنوي .390	لم يكن هناك فرق معنوي بين أحكام الذكور على مستوى بديلي الإفصاح
الإناث	معنوي .001	كان للإفصاح من خلال تقرير منفصل أكثر معنوية على أحكام الإناث مقارنة بتقرير مجلس الإدارة	معنوي .015	كان للإفصاح من خلال تقرير منفصل أكثر معنوية على أحكام الإناث مقارنة بتقرير مجلس الإدارة	غير معنوي .152	لم يكن هناك فرق معنوي بين أحكام الإناث على مستوى بديلي الإفصاح

جدول رقم (36)
ملخص نتائج **الأثر المعدل لعمر المشاركين** (ملخص نتائج **فرض الدراسة الثالث**)

(أ) الإفصاح من خلال تقرير مجلس الإدارة (H3a)

	أحكام المستثمرين بخصوص تقييم السهم			أحكام المستثمرين بشأن قرار الاستثمار			أحكام العملاء بشأن التعامل في خدمات البنك الالكترونية		
	الأكبر سنا	الأصغر سنا	تفسير النتيجة	الأكبر سنا	الأصغر سنا	تفسير النتيجة	الأكبر سنا	الأصغر سنا	تفسير النتيجة
أثر الإفصاح	معنوي .000	غير معنوي .132	كان تأثير الإفصاح على تقييم سعرالسهم معنوياً للأكبر سنا فقط	معنوي .000	غير معنوي .129	كان تأثير الإفصاح على الاستثمار معنوياً للأكبر سنا فقط	معنوي .021	غير معنوي .078	كان تأثير الإفصاح على قرار التعامل في الخدمات الالكترونية معنوياً للأكبر سناً والأصغر سنا
معنوية الفرق بين الأصغر والأكبر سنا	معنوي .001		يوجد فرق معنوي بين أحكام الأكبر والأصغر سناً عند تلقي الإفصاح من خلال تقرير مجلس الإدارة	غير معنوي .007		هناك فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير مجلس الإدارة	غير معنوي .078		لا يوجد فرق معنوي بين قرارات الذكور أو الإناث للتعامل على الخدمات الالكترونية للبنك عند الحصول على الإفصاح من خلال تقرير مجلس الإدارة

(ب) الإفصاح من خلال تقرير منفصل (H3b)

	أحكام المستثمرين بخصوص **تقييم السهم**			أحكام المستثمرين بشأن **قرار الاستثمار**			أحكام العملاء بشأن **التعامل في خدمات البنك الالكترونية**		
	الأكبر سنا	الأصغر سنا	تفسير النتيجة	الأكبر سنا	الأصغر سنا	تفسير النتيجة	الأكبر سنا	الأصغر سنا	تفسير النتيجة
أثر الإفصاح	معنوي .004	معنوي .007	كان تأثير الإفصاح على تقييم سعرالسهم معنوياً لكل من الأكبر والأصغر سنا	معنوي .000	معنوي .005	كان تأثير الإفصاح على الاستثمار معنوياً فقط لكل من الأكبر والأصغر سنا	معنوي .001	معنوي .000	كان تأثير الإفصاح على قرار التعامل على الخدمات الالكترونية معنوي على مستوى الأكبر والأصغر سنا
معنوية الفرق بين الأصغر والأكبر سنا	غير معنوي .199		لا يوجد فرق معنوي بين أحكام الأكبر والأصغر سناً عند تلقي الإفصاح من خلال تقرير منفصل	معنوي .004		يوجد فرق معنوي بين أحكام الذكور والإناث عند تلقي الإفصاح من خلال تقرير منفصل	غير معنوي .197		لا يوجد فرق معنوي بين قرارات الذكور أو الإناث للتعامل على الخدمات الالكترونية للبنك عند الحصول على الإفصاح من خلال تقرير منفصل

(ج) الفرق بين معنوية أحكام المشاركين من خلال بديلي الإفصاح على مستوى كل من الأكبر والأصغر سناً (H3c)

	أحكام المستثمرين بخصوص **تقييم السهم**		أحكام المستثمرين بشأن **قرار الاستثمار**		أحكام العملاء بشأن **التعامل في خدمات البنك الالكترونية**	
	P-value	تفسير النتيجة	P-value	تفسير النتيجة	P-value	تفسير النتيجة
الأكبر سنا	معنوي .032	هناك فرق معنوي بين أحكام الأكبر سنا باختلاف بديلي الإفصاح	غير معنوي .376	لم يكن هناك فرق معنوي بين أحكام الأكبر سنا على مستوى بديلي الإفصاح	غير معنوي .448	لم يكن هناك فرق معنوي بين أحكام الأكبر سنا على مستوى بديلي الإفصاح
الأصغر سنا	غير معنوي .004	هناك فرق معنوي بين أحكام الأصغر سنا باختلاف بديلي الإفصاح	معنوي .002	هناك فرق معنوي بين أحكام الأصغر سنا باختلاف بديلي الإفصاح	غير معنوي .887	لم يكن هناك فرق معنوي بين أحكام الأصغر سنا على مستوى بديلي الإفصاح

12- نتائج الدراسة والتوصيات ومجالات البحث المقترحة:

استهدف البحث اختبار أثر بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني بالبنوك على أحكام كل من المستثمرين والعملاء، واختبار الأثر المعدل للخصائص الديموغرافية للمشاركين على تلك النتائج مع التركيز عل كل من الجنس والعمر. ومن خلال دراسة تجريبية **توصل البحث** إلى عدد من النتائج أهمها: أن كل من بديلي الإفصاح عن إدارة مخاطر الأمن السيبراني له تأثير معنوي على كل من تقييم المستثمرين للأسهم، وقرار الاستثمار في الأسهم، وقرار العملاء بالتعامل على الخدمات الالكترونية للبنك واستخدام بطاقات الائتمان للتعامل عبر الانترنت (وهو ما يدعم فرض الدراسة الأول بفرعياته الأولى والثانية)، ولاختبار الأثر التفاضلي بين بديلي الإفصاح (فرض الدراسة الفرعي الثالث من الفرض الأول) توصل البحث إلى أن الإفصاح من خلال تقرير منفصل له تأثير أكثر معنوية على تقييم الأسهم، واتخاذ قرار الاستثمار مقارنة بالإفصاح من خلال تقرير مجلس الإدارة، غير أنه لم يكن هناك فرقاً معنوياً بين بديلي الإفصاح بخصوص قرار العملاء بشأن الخدمات الالكترونية للبنك، بما يشير إلى اهتمام العملاء بالمعلومات المقدمة عن إدارة المخاطر السيبرانية وأخذها في الاعتبار عند قرار التعامل على الخدمات الالكترونية بغض النظر عن طريقة تقديم تلك المعلومات.

وبإجراء **تحليل حساسية** على فئة الأكاديميين توصلت الدراسة إلى أن بديل الإفصاح من خلال تقرير مجلس الإدارة لم يكن له تأثيراً معنوياً على أحكام تقييم الاسهم أو قرارات الاستثمارات، في حين كان لبدل الإفصاح من خلال تقرير منفصل أثراً معنوياً على تقييم الأسهم وقرار الاستثمار. وأن كلا بديلي الإفصاح كان له تأثيراً معنوياً على قرارات العملاء للتعامل في الخدمات الالكترونية. وتشير تلك النتيجة إلى أن الإفصاح من خلال تقرير مجلس الإدارة لم يكن له تأثيراً معنوياً على الاكاديميين فيما يتعلق بقرار الاستثمار، بينما اهتم المهنيين بذلك الإفصاح من خلال تقرير مجلس الإدارة وأدى إلى التأثير المعنوي على أحكام الاستثمار الخاصة بهم، في حين أن الإفصاح من خلال تقرير منفصل كان له محتوى معلوماتي هام لكل من الأكاديميين والمهنيين.

كما توصلت نتائج اختبار فرض الدراسة الثاني إلى أن الإفصاح **من خلال تقرير مجلس الإدارة** له تأثير معنوي على قرارات الاستثمار المتعلقة بتقييم الاسهم وقرار الاستثمار في السهم وذلك للذكور فقط ولم يكن له تأثير على قرارات الاستثمار الخاصة بالإناث، إلا أنه كان له تأثير معنوي على قرارات الذكور والإناث الخاصة بالتعاملات على الخدمات الالكترونية للبنك (كعملاء) وكان الفرق بين قرارات الذكور والإناث غير معنوي فيما يتعلق بقرار التعامل مع خدمات البنك الالكترونية. أما فيما يتعلق بالإفصاح **من خلال تقرير منفصل** كان له تأثير معنوي على قرارات الاستثمار المتعلقة بتقييم الاسهم وقرار الاستثمار في السهم وقرار التعامل في الخدمات الالكترونية للبنك لكل من الذكور والإناث. وكان الفرق بينهما غير معنوي فيما يتعلق بتقييم الأسهم وقرار الاستثمار (كمستثمرين)، أما قرار التعامل في خدمات البنك الالكترونية فكان الفرق بين الذكور والإناث غير معنوي. كما أشارت الاختبارات

إلى أن **الإفصاح من خلال تقرير منفصل مقارنة بالإفصاح من خلال تقرير مجلس الإدارة** لم يكن له تأثير معنوي على أحكام الذكور، بينما كان معنوياً على مستوى الإناث فيما يتعلق فقط بقرارات تقييم الأسهم والاستثمار ولم يكن معنوياً فيما يتعلق بقرار التعامل مع خدمات البنك الالكترونية. وبذلك يتم قبول فرض الدراسة الفرعي (H2a) على مستوى قرارات الاستثمار دون قرارات التعامل في الخدمات الالكترونية للبنك. وقبول فرض الدراسة الفرعي (H2b) على مستوى قرارات التعامل في الخدمات الالكترونية للبنك دون قرارات الاستثمار. يتم قبول فرض الدراسة الفرعي (H2c) على مستوى قرارات الاستثمار دون قرارات التعامل في الخدمات الالكترونية للبنك.

وأشار **تحليل الحساسية** على عينة الأكاديميين، إلى عدم وجود تأثير معنوي للإفصاح من خلال تقرير مجلس الإدارة على مستوى أي من الذكور أو الإناث، فيما يتعلق بقرارات الاستثمار، وكان التأثير معنوياً لدى كل من الذكور أو الإناث فيما يتعلق بقرارات التعامل مع الخدمات الالكترونية للبنك. أما على مستوى الإفصاح من خلال تقرير منفصل فقد جاءت النتائج تشير إلى وجود أثر معنوي على أحكام كل من الذكور والإناث سواء تقييم الأسهم أو الاستثمار أو التعامل في الخدمات الالكترونية للبنك. إضافة لعدم وجود فرق معنوي بين أحكام الذكور أو الإناث سواء قبل الحصول على الإفصاح عن إدارة مخاطر الأمن السيبراني أو بعد الحصول على الإفصاح عن مخاطر الأمن السيبراني. وتشير تلك النتائج إلى أن الجنس ليس له تأثير معنوي على العلاقة بن بديلي الإفصاح عن مخاطر الأمن السيبراني وبين أحكام المشاركين من الأكاديميين.

أما نتائج اختبار فرض الدراسة الثالث فتوصلت إلى أن الإفصاح **من خلال تقرير مجلس الإدارة** له تأثير معنوي على كافة قرارات الاستثمار وقرار التعامل في الخدمات الالكترونية فقط لكبار السن وليس لصغار السن، بما يشير إلى أن كبار السن فقط يجدون محتوى معلوماتي في للإفصاح عن إدارة مخاطر الأمن السيبراني ضمن تقرير مجلس الإدارة. أما فيما يتعلق بالإفصاح **من خلال تقرير منفصل** فقد كان له تأثير معنوي على قرارات الاستثمار المتعلقة بتقييم الاسهم وقرار الاستثمار في السهم لكل من كبار السن وصغار السن معاً بما يشير إلى استفادة جميع الفئات العمرية من الإفصاح عن مخاطر الأمن السيبراني ضمن تقرير منفصل. كما أشارت الاختبارات إلى أن **الإفصاح من خلال تقرير منفصل مقارنة بالإفصاح من خلال تقرير مجلس الإدارة** كان له تأثير معنوي على أحكام الأصغر سناً فيما يتعلق بقرارات تقييم الأسهم والاستثمار، دون قرار التعامل في الخدمات الالكترونية، بينما لم يكن هناك فرقاً معنوياً لبديلي الإفصاح على قرارات الأكبر سناً إلا فقط فيما يخص تقييم السهم. وبالتالي يمكن القول أن عامل العمر له أثر معدل على العلاقة بين بديل الإفصاح وقرارات الاستثمار دون قرار التعامل على الخدمات الالكترونية للبنك.

وأشارت **نتائج تحليل الحساسية** على الأكاديميين بأن الإفصاح عن إدارة مخاطر الأمن السيبراني عبر تقرير مجلس الإدارة يؤدي إلى تحسن قرارات العملاء دون أن يؤثر معنوياً على قرارات تقييم الأسهم والاستثمار،

وذلك على مستوى الأكبر سناً والأصغر سناً للأكاديميين. أما على مستوى الإفصاح من خلال تقرير منفصل فقد جاءت النتائج تشير إلى وجود أثر معنوي على أحكام الأكبر سناً والأصغر سناً فيما يتعلق بقرارات العملاء بالتعامل في الخدمات الالكترونية، أما فيما يتعلق بقرارات تقييم الأسهم والاستثمار فقط كانت الإفصاح ضمن تقرير منفصل له أثر معنوي على أحكام المستثمرين الأكبر سنا وليس الأصغر سناً. وتؤكد تلك النتائج على أن العلاقة بين الإفصاح عن إدارة مخاطر الأمن السيبراني وقرارات المتعاملين تتأثر بعامل العمر.

وفي ضوء ما تم التوصل اليه من نتائج **فإن الباحث يوصي** بأن تعمل هيئة الرقابة المالية على توفير إطار منظم للإفصاح عن معلومات إدارة الأمن السيبراني، لما لها من أهمية للمستخدمين تمكنهم من إدراك قدرة الشركات (لاسيما البنوك) في تأمين أنظمتها وقدرتها على التعامل مع التهديدات السيبرانية. كما يمكن أن يسهم أيضاً في ذلك الدور البنك المركزي باعتباره المنوط به تنظيم وإدارة عمل البنوك بمصر. كما يوصي الباحث بأن يتم تضمين الأمن السيبراني ومخاطره وكيفية إدارة تلك المخاطر، وإعداد تقارير الأمن السيبراني ضمن مقرر نظم المعلومات المحاسبية بمناهج أقسام المحاسبة بكليات التجارة.

كما يفتح هذا البحث المجال **للعديد من البحوث المستقبلية** ومنها؛ اختبار علاقة الإفصاح عن مخاطر الأمن السيبراني، والإفصاح عن إدارة محاطر الأمن السيبراني بمخاطر واتعاب المراجعة، فمن المتوقع وفقاً لأدبيات تقدير خطر المراجعة وانعكاسها على اتعاب المراجعة، أن تقدير المراجع لمخاطر التقاضي يمكن أن يؤثر بشكل معنوي على حجم ونطاق إجراءات المراجعة، وهو ما ينعكس على حكمه بشأن الأتعاب المراجعة. كما يمكن إعادة اختبار فروض الدراسة ولكن مع تصميم للحالة يتضمن الإفصاح عن تعرض الشركة لمخاطر واختراقات سيبرانية. كذلك يمكن إجراء دراسة لاختبار أثر التعرض لاختراقات سابقة على سلوك الشركة للإفصاح عن إدارة مخاطر الأمن السيبراني. كما يمكن أيضاً اختبار أثر تعرض الشركة للاختراقات على أسعار الأسهم والدور المعدل للإفصاح السابق عن المخاطر المحتملة على تلك العلاقة.

قائمة المراجع

أولاً المراجع العربية:

أبو الخير، محمد حارس محمد طه. 2022. أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية. ***المجلة العلمية للدراسات والبحوث المالية والإدارية***. العدد الأول، مارس، المجلد الخامس عشر. صـ صـ 1-71.

الاتحاد المصري للتأمين. 2019. الهجمات الالكترونية (السيبرانية) والتأمين. عدد أسبوعي رقم 67. https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

البغدادي، مروة فتحي السيد. 2021. اقتصاديات الأمن السيبراني في القطاع المصرفي. ***مجلة البحوث القانونية والاقتصادية***. العدد 76: 1447-1513.

الخرينج، نواف متعبنية متعب، داو، ياسر ابراهيم، عبد الرحمن، مروة أحمد. 2022. دور حوكمة تكنولوجيا المعلومات في إدارة الخاطر السيبرانية للقطاع المصرفي. . ***المجلة العلمية للدراسات والبحوث المالية والإدارية***. كلية التجارة، جامعة مدينة السادات. العدد الثاني، مارس، المجلد الثاني عشر. صـ صـ 1715- 1743.

الرشيدي، طارق عبد العظيم يوسف، وناصر، داليا عباس السيد. 2019. أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات. ***مجلة المحاسبة والمراجعة***. جامعة بني سويف، كلية التجارة. العدد الثاني. صـ صـ 439-487. https://doi.org/10.21608/NAUS.2019.92313

السجيني، صبري عبد الحميد، عبد الرازق، دينا سمير، عياده، طيف خضر. 2023. دور إطار COBIT2019 في إدارة مخاطر عمليات تكنولوجيا المعلومات بالمصارف العراقية- دراسة ميدانية. ***المجلة المصرية للدراسات التجارية***. العدد الثاني، المجلد 47. صـ صـ 318-343.

المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء. الاستراتيجية الوطنية للأمن السيبراني 2017-2021، والمحدثة بالاستراتيجية الوطنية للأمن السيبراتي 2023-2027. https://mcit.gov.eg/ar/Publication/Publication_Summary/10492

الهيئة الوطنية للأمن السيبراني. 2020. المملكة العربية السعودية. https://www.nca.gov.sa/national_cybersecurity_strategy-ar.pdf

شحاته، شحاته السيد. 2022. نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية. ***المجلة العلمية للدراسات والبحوث المالية والإدارية***. كلية التجارة، جامعة مدينة السادات. العدد الثاني، مارس، المجلد الثالث عشر. صـ صـ 26- 37.

شرف، إبراهيم أحمد ابراهيم. 2023. أثر إفصاح الشركات عن تقرير إدارة لمخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين: دراسة تجريبية. ***مجلة الاسكندرية للبحوث المحاسبية***. قسم المحاسبة والمراجعة، كلية التجارة، جامعة الاسكندرية.العدد الأول، يناير، المجلد السابع. صـ صـ 211-281. https://search.mandumah.com/Record/1370433

صندوق النقد العربي. 2019. **موجز السياسات حول أمن الفضاء السيبراني في القطاع المصرفي**. العدد الرابع: 8-7-2019.

عثمان، محمد أحمد عبد العزيز. 2023. أثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم- درسة تجريبية. ***مجلة الإسكندرية للبحوث المحاسبية***. قسم المحاسبة والمراجعة، كلية التجارة، جامعة الاسكندرية. العدد الثاني، مايو، المجلد السابع .صـ صـ 167-238.

عزام، عبد المرضي حامد، يحيى سعد زغلول، 2006، **الاستدلال الإحصائي: مدخل إلى اتخاذ القرار والتنبؤ**، قسم الإحصاء والرياضة والتأمين، كلية التجارة، جامعة الإسكندرية

عطية، أحمد محمد صلاح. 2021. التحول الرقمي في مصر هل يلقي بمسئوليات جديدة على المراجع؟. ***مجلة البحوث التجارية***. العدد الأول، المجلد 43: صـ صـ 51-65.

على، محمود أحمد وعلي، صالح علي صالح. 2022. 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، كلية التجارة، جامعة الاسكندرية. العدد الثالث، سبتمبر، المجلد السادس.صـ صـ 1-48.

فريد، حنان فريد. 2022. الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية دراسة تجريبية. العدد الرابع، اكتوبر، المجلد الثالث عشر. صـ صـ 412-488. doi:10.21608/jces.2022.285187
https://jces.journals.ekb.eg/article_285187_2e4a3415b248d1c893cf92f55dd1da1b.pdf

قانون البنك المركزي والجهاز المصرفي الصادر بالقانون رقم 194 لسنة 2020. https://drive.google.com/file/d/1R0Pt4JRf_KJaOC_d-gdri9UuU-SpARYw/view?usp=sharing

قانون تنظيم وتنمية استخدام التكنولوجيا المالية في الأنشطة المالية غير المصرفية الصادر بالقانون رقم 5 لسنة 2022. https://fra.gov.eg/wp-content/uploads/2022/02/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AA%D9%86%D8%B8%D9%8A%D9%85-%D9%88%D8%AA%D9%86%D9%85%D9%8A%D8%A9-_unlocked.pdf

قرار الهيئة العامة للرقابة المالية رقم 139 لسنة 2023 بشأن التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين، وذلك لمزاولة أنشطة الخدمات المالية غير المصرفية. https://fra.gov.eg/wp-content/uploads/2023/07/%D9%86%D8%B4%D8%B1-%D9%82%D8%B1%D8%A7%D8%B1-%D8%B1%D9%82%D9%85-139-%D9%84%D8%B3%D9%86%D8%A9-2023-%D8%A8%D8%A7%D9%84%D9%88%D9%82%D8%A7%D8%A6%D8%B9.pdf

كتاب دوري رقم (3) لسنة 2024 الصادر في 10-7-2024 عن الهيئة العامة للرقابة المالية بشأن إجراءات تعزيز الأمن السيبراني في مؤسسات قطاع التمويل غير المصرفي. https://fra.gov.eg/wp-content/uploads/2024/07/Document.pdf

كعموش، شريف علي خميس ابراهيم. 2018. أثر توكيد مراقب الحسابات على الإفصاح عن رأس المال الفكري على أحكام المستثمرين – دراسة تجريبية. ***مجلة الاسكندرية للبحوث المحاسبية***. قسم المحاسبة والمراجعة- كلية التجارة جامعة الاسكندرية. العدد الثاني، ديسمبر، المجلد الثاني. صـ صـ 98-1. doi:10.21608/aljalexu.2018.58050 https://aljalexu.journals.ekb.eg/article_58050_05a3b2152710d0a950394cc42f2726d7.pdf

محمد، ممدوح عبد الفتاح أحمد، 2021. العوامل المؤثرة والمعيقة لتبني العملاء للخدمات الممصرفية الإلكترونية: دراسة ميدانية مقارنة بين عملاء المصارف السعودية والمصرية. ***المجلة العربية للإدارة***. العدد الرابع، المجلد 41. صـ صـ 257-223.

موسى، سعاد زغلول، 2018، "**أثر توكيد المراجع الخارجي على تقارير الأعمال المتكاملة على قراري الاستثمار ومنح الائتمان- دراسة تجريبية**"، رسالة دكتوراه غير منشورة كلية التجارة، جامعة الإسكندرية.

يوسف، أماني أحمد وهبة. 2022. واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة: دراسة تجريبية. ***المجلية العلمية للدراسات التجارية والبيئية***. العدد الثاني عشر ابريل المجلد الثالث. صـ صـ 28- 109. *https://doi.org/10.21608/jces.2022.248639*

ثانياً المراجع الأجنبية:

Agarwal, R., Rastogi, S. and Mehrotra, A. 2009. Customers' perspectives regarding e-banking in an emerging economy. ***Journal of Retailing and Consumer Services***. 16(5): 340-351. *https://doi.org/10.1016/j.jretconser.2009.03.002*

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

Al-Alawi, A. I. and Al-Bassam, S. A. 2020. The significance of cybersecurity system in helping. ***Journal of Xidian University***. 14(7): 1523-1536. *https://doi.org/10.37896/jxu14.7/174*

Ali, S. E. A., Lai, F.-W., Aman, A., Saleem, M. F., and Hamad, S. (2022). Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk? ***Journal of Competitiveness***. 14(1): 23–42. *https://doi.org/10.7441/joc.2022.01.02*

Amir, E., Levi, S., & Livne, T. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. ***Review of Accounting Studies***. 23 (3): 1177-1206. *doi:10.1007/s11142-018-9452-4*

Bucsa, R.C. 2021. Risk management in information security. ***Economy Transdisciplinarity Cognition.*** 24 (1): 50-55.

Cains, M. J., Flora, L., Taber, T., King, Z. and Henshel, D. S. 2022. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. 2022. ***Risk Analysis***, 42(8): 1643-1669. *doi: 10.1111/risa.13687*

Chen, J., Henry, E. and Jiang, X. 2023. Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. ***Journal of Business Ethics***. 187: 199–224. *https://doi.org/10.1007/s10551-022-05107-z*

Cheong, A., Yoon, K., Cho, S., and No, W. G. 2021. Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. ***Journal of information Systems***. 35 (2): 179-194. *https://doi.org/10.2308/ISYS-2020-031*

Choo, K. K. R. 2011. The cyber threat landscape: Challenges and future research directions. ***Computers and Security***. 30(8): 719-731. *https://doi.org/10.1016/j.cose.2011.08.004*

Coram, P. 2009. The effect of investor sophistication on the influence of nonfinancial performance indicators on investors' judgments. ***Accounting and Finance.*** 50(2):263-280. *http://dx.doi.org/10.2139/ssrn.1468145*

Coram, P., Monroe, G. S. and Woodliff, D. R. 2009. The value of assurance on voluntary nonfinancial disclosure: An experimental evaluation. ***Auditing: A Journal of Practice and Theory***. 28(1): 137-151. *http://dx.doi.org/10.2308/aud.2009.28.1.137*

Cortez, E. K. and Dekker, M. 2022. A Corporate governance approach to cybersecurity risk disclosure. ***European Journal of Risk Regulation.*** 13: 443–463. *doi:10.1017/err.2022.10*

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. *https://doi.org/10.17705/1jais.00740*

Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O. and Ewuga, S. K. 2023. Cybersecurity risk assessment in banking: methodologies and best practices. ***Computer***

Science And It Research Journal, 4(3), 220-243. *https://doi.org/10.51594/csitrj.v4i3.659*

Dodla, T. R. and Jones, L. A. 2023. Mitigating knowledge management Internal and external risk factors: A literature review of best practices. **Buletin Ştiinţific.** 1(55): 45- 54. *https://doi.org/10.2478/bsaft-2023-0005*

Elena-Bucea, A., Cruz-Jesus, F., Oliveira, T., and Coelho, P. S. 2021. Assessing the role of age, education, gender and income on the digital divide: Evidence for the European Union. ***Information Systems Frontiers***. *23*: 1007-1021. *https://doi.org/10.1007/s10796-020-10012-9*

Faisal, F., Abidin, Z. and Haryanto, H. 2021. Enterprise risk management (ERM) and firm value: The mediating role of investment decisions. ***Cogent Economics and Finance***. 9:1-15. *DOI: 10.1080/23322039.2021.2009090 https://doi.org/10.1080/23322039.2021.2009090*

Firoozi, M. and Mohsni, S. 2023. Cybersecurity disclosure in the banking industry: a comparative study. ***International Journal of Disclosure and Governance***. 20: 451–477. *https://doi.org/10.1057/s41310-023-00190-8*

Frank, M. L., Grenier, J. H. and Pyzoha, J.S. 2019. How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance. ***Journal of Information Systems.*** 33 (3): 83–200. *http://dx.doi.org/10.2308/isys-52374*

Frank, M. L., Grenier, J. H. and Pyzoha, J.S. 2023. Implications of Enhanced Cybersecurity Risk Management Reporting and Independent Assurance. ***Current Issues in Auditing.*** 17(1): 11-18. *doi: 10.2308/ciia-2022-018*

Friedmann, E. and Lowengart, O. 2016. The effect of gender differences on the choice of banking services. ***Journal of Service Science and Management***. 9: 361-377. *doi: 10.4236/jssm.2016.95041*

Gao, L., Calderon, T. G., and Tang, F. 2020. Public companies' cybersecurity risk disclosures. ***International Journal of Accounting Information Systems***. 38 . *https://doi.org/10.1016/j.accinf.2020.100468*

Gatzert, N. and Schubert, M. 2022. Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. ***Journal of Risk and Insurance***. 89:725–763. *https://doi.org/10.1111/jori.12381*

Goel, S. and Shawky, H. A. 2023. Estimating the market impact of security breach announcements on firm values. ***Information and Management***. 46(7): 404-410. *https://doi.org/10.1016/j.im.2009.06.005*

Haddad, A. E. and Alali, H. 2022. Risk disclosure and financial performance: The case of Islamic and conventional banks in the GCC. ***Journal of Islamic Accounting and Business Research***. 13(1): 54-72. *https://doi.org/10.1108/JIABR-11-2020-0343*

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M. and Dawodu, S. O. 2024. ***Computer Science and IT Research Journal***. (5)1: 41-59. https://doi.org/*10.51594/csitrj.v5i1.701*

Hishleifer, D and Teoh, S H. 2003. Limited attention, information disclosure, and financial reporting. ***Journal of Accounting and Economics***. 36: 337-386. *https://doi.org/10.1016/j.jacceco.2003.10.002*

IBM Security. 2023. Cost of a data breach report. *https://www.ibm.com/reports/data-breach*

IMFBlog, International monetary fund. 2024. *https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability*

Iqbal, J., Sohail, M. K., Irshad, A. and Khan, R. A. 2024. Risk management disclosures and banks financial performance: evidence from emerging markets. ***Risk Management***. 26(1):1-21. *https://doi.org/10.1057/s41283-023-00136-y*

ITU (International Telecommunication Union). 2010-2011. Trends in Telecommunications reform 2010-2011. *https://www.academia.edu/9263005/Trends_in_Telecommunications*

Izogo, E., Nnaemeka, O. C., Onuoha, O. A. and Ezema, K. S. 2012. Impact of demographic variables on consumers' adoption of E-banking in Nigeria: An empirical investigation. ***European Journal of Business and Management***. 4(17): 27-39. *https://www.researchgate.net/publication/283504884_Impact_of_Demographic_Variables_on_Consumers'_Adoption_of_E-banking_in_Nigeria_An_Empirical_Investigation*

Jain, D. and Mandot, N. (2021). Impact of demographic factors on investment decision of investors in Rajasthan. ***Researchers World - International Refereed Social Sciences Journal***. 3(2(3), 81–92. *https://www.researchersworld.com/index.php/rworld/article/view/617*

Janvrin, D. J. and Wang, T. 2022. Linking cybersecurity and accounting: an event, impact, response framework. ***Accounting Horizons***. 36(4): 67-112. *doi: 10.2308/horizons-2020-101*

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. *https://doi.org/10.2308/ISYS-2020-067*

Kelton, A. S. 2021. How to reduce the cybersecurity breach contagion effect. ***Current Issues in Auditing***. 15 (2): 1-9. *https://doi.org/10.2308/CIIA-2020-025*

Kelton, A. S., 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*

Kelton, A. S., and Pennington, R. R. and Tuttle, B. M. 2010. The effect of information presentation format on judgement and decision making: A review of information system research. ***Journal of Information System***. 24(2): 79-105. *https://doi.org/10.2308/jis.2010.24.2.79*

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/*

Korniotis, G. M. and Kumar, A. 2011. Do older investors make better investment decisions?. *The* ***Review of Economics and Statistics.*** 93 (1): 244–265. *https://doi.org/10.1162/REST_a_00053*

Luo, Y. and Salterio, S.E. 2022. The Effect of Gender on Investors' Judgments and Decision-Making. ***Journal of Business Ethics***. 179, 237–258 (2022). *https://doi.org/10.1007/s10551-021-04806-3*

Mauldin, E. and Arunachalam, V. 2002. An experimental examination of alternative forms of web assurance for business-to-customer e-commerce. ***Journal of Information Systems***. 16: 33-54. *http://dx.doi.org/10.2308/jis.2002.16.s-1.33*

McKinsey. 2024. Cyber War is Just around: Strategies to reduce emerging technology risks in financial services companies, 11 March 2024, report. *https://www.mckinsey.com/featured-insights/highlights-in-arabic/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services-arabic/ar*

Melaku, H. M. 2023. Context-based and adaptive cybersecurity risk management framework. ***Risks***. 11 (101): 1-22. *https://doi.org/10.3390/risks11060101*

Metawa, N., Hassan, M.K., Metawa, S. and Safa, M.F. 2019. Impact of behavioral factors on investors' financial decisions: case of the Egyptian stock market. ***International Journal of Islamic and Middle Eastern Finance and Management***. 12 (1)1: 30-55. *https://doi.org/10.1108/IMEFM-12-2017-0333*

Niessen-Ruenzi, A. and Zimmerer, L. 2024. The Gender Investment Gap: Reasons and Consequences. Working Paper, available at: *https://ssrn.com/abstract=4692726*

Obamuyi, T.M., 2013. Factors influencing investment decisions in capital market: A study of individual investors in Nigeria. ***Organizations and Markets in Emerging Economies.*** 4 (7): 141-161. *http://dx.doi.org/10.15388/omee.2013.4.1.14263*

Proofpoint. 2023. Threat report 2023 ponemon healthcare cybersecurity report. *https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report#:~:text=Here%20are%20just%20a%20few,in%20the%20past%20two%20years*

Reimsbach, D. and Hahn, R. 2017. Integrated Reporting and Assurance of Sustainability Information: An Experimental Study on Professional Investors' Information Processing. ***European Accounting Review.*** **Available on line at:** *https://www.researchgate.net/publication/311495130*

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*

Sevilla, I. S. 2021. Framing and governing cyber risks: comparative analysis of U.S. Federal policies [1996–2018]. ***Journal of Risk Research***. 24(6): 692–720. *https://doi.org/10.1080/13669877.2019.1673797*

Shah, P. 2023. The role of gender factor in investment decisions. 2023. ***International Journal of Creative Research Thoughts***. 11 (6): 667-670. https://ijcrt.org/papers/IJCRT2306406.pdf

Shaik, G. M., Katpar, N. K., Kalhoro, M. Abro, Y.K. and Phanwar, G. A. 2019. Do behavioral biases in gender differences affect investment decisions? ***Sociology International Journal***. 3 (4): 326-336. *https://doi.org/10.15406/sij.2019.03.00194*

Shen, H. Huiying Wu, H. and Chand, P. 2017. The impact of corporate social responsibility assurance on investor decisions: Chinese evidence. ***International Journal of Audit***. 21: 271-287. *http://dx.doi.org/10.1111/ijau.12094*

Siraji, M., Nazar, M. and Ali, I. 2021. Irrational Behaviour and Stock Investment Decision. Does Gender Matter? ***Revista GEINTEC.*** 11 (2): 2185-2204. Electronic copy available at: *https://ssrn.com/abstract=3910478*

Stanikzai, A.Q. and Shah, M. A. 2021. Evaluation of cyber security threats in banking systems. 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA. 1-4. *https://doi.org/10.1109/SSCI50451.2021.9659862*

Teimoor, R. A. 2021. A review of database security concepts, risks, and problems. ***Journal of Science and Technology***. 5(2): 38-46. *doi: 10.21928/uhdjst.v5n2y2021*

Tosun, O. K. 2021. Cyber-attacks and stock market activity. ***International Review of Financial Analysis***. 76. *https://doi.org/10.1016/j.irfa.2021.101795*

Walton, S., Wheeler, P. R., Zhang, Y. I., and Zhao, X. R. 2021. An integrative review and analysis of cybersecurity research: Current state and future directions. ***Journal of Information Systems***. 35 (1): 155-186. *https://doi.org/10.2308/ISYS-19-033*

Wang, F., Wu, C., Liu, L., Zhao, J. and Zhang, Y. 2023. Research on Pest. CRITIC-EMG(1,1) method for security risk warning of regional digital economy. The Journal of Grey System. 35 (1): 49-66. *http://www.researchinformation.co.uk/*

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. https://doi.org/10.1108/IJAIM-02-2019-0022

Yuen, Y. Y. 2013. Gender and Age Effect on Acceptance of Internet Banking: Cultural Comparison between United States and Malaysia. International Journal of Business and Management. 8 (18): 1-11. *http://dx.doi.org/10.5539/ijbm.v8n18p1*

Zbar, Z. A. 2022. The Development of The Management A Digital Risks To Face The Risk Of Using It In A Sample Of Iraqi Bank. ***Webology.*** 8 (3): 1389-1407. *https://www.webology.org/data-cms/articles/20220524100023pmwebology%2019%20(3)%20-%2096%20pdf.pdf*

Zwane, S., Wannenburg, E. and De Jager, J. 2023. Gender differences and the usage of online banking services in Swaziland. **Journal of Business and Social Review in Emerging Economies**. *9* (3): 233-244. *https://doi.org/10.26710/jbsee.v9i3.2699*

الملاحق

الحالة التجريبية

جامعة الإسكندرية
كلية الأعمال (التجارة سابقاً)
قسم المحاسبة والمراجعة

الأستاذ الفاضل/.....

تحية طيبة وبعد،،

يقوم الباحث بإعداد بحث في مجال الإفصاح الاختياري عن إدارة مخاطر الأمن السيبراني. وتمثل الحالة المقدمة لسيادتكم أهم أدوات البحث لتجميع البيانات لغرض اختبار فروض الدراسة.

ويتقدم الباحث لسيادتكم مقدماً بخالص الشكر والتقدير لحسن تعاونكم ومساهمتكم الفعالة في إنجاز ذلك البحث من خلال الاجابة على كافة الأسئلة المرفقة بالحالة المقدمة لسيادتكم. ويؤكد الباحث لسيادتكم أن إجاباتكم على تلك الأسئلة تحظى بالسرية التامة ولن تستخدم إلا لغرض البحث العلمي فقط.

وتفضلوا سيادتكم بقبول فائق الاحترام والتقدير،،

الباحث

أولاً البيانات الشخصية

1- الاسم (اختياراً)/ .....

2- الوظيفة الحالية/ .....

3- جهة العمل/ .....

4- العمر/ ..... سنة

5- الجنس/ أ- ذكر ب- أنثى

6- المؤهل الدراسي/ أ- بكالوريوس ب- دبلومة ج- ماجستير د- دكتوراه

7- شهادات مهنية (إذا وجدت)/

1- ..... 2- ..... 3- ..... 4- .....

8- عدد سنوات الخبرة في العمل: ..... سنة

نبذة عن أهم المصطلحات في الدراسة:

اهتم الفكر المحاسبي في الآونة الأخيرة بقضية مخاطر الأمن السيبراني، وإدارة تلك المخاطر من قبل إدارة الشركات، لاسيما في تلك الشركات التي تعمل في بعض القطاعات ذات المخاطر السيبرانية المرتفعة (مثل البنوك، وشركات التكنولوجيا، والتأمين....)، وقد لاقى موضوع إفصاح الشركات عن كيفية إدارة الخطر السيبراني المزيد من الاهتمام من قبل الباحثين، من حيث تأثير ذلك الإفصاح، وأكدت الدراسات في هذا المجال على أن إدارة المخاطر السيبرانية تؤدى إلى نجاح أو فشل المنشآت في تحقيق أهدافها، حيث أنه يسهم بقوة في تعزيز القدرة على الاستمرار في المستقبل خاصة للمنشآت التي تعمل فيما يعرف بيئة الاقتصاد القائم على المعرفة والتكنولوجيا.

وقد ظهر الاهتمام بالتقرير عن مخاطر الأمن السيبراني وإدارتها نتيجة الفجوة بين ما يمكن أن تقدمه القوائم المالية من إفصاحات كافية بشأن تلك المخاطر وإدارتها وانعكاسها على القوائم المالية للشركات. حيث قد لا تعكس القوائم المالية في غالبية الأحيان قدرة الشركة على إدارة مخاطر الأمن السيبراني، إذ تركزت الإفصاحات ضمن الإيضاحات بالقوائم المالية على قدرة الشركة على إدارة المخاطر المالية مثل مخاطر الائتمان، والتقلب في سعر الصرف، والسيولة. الأمر الذي فتح الباب إلى الافصاح الاختياري عن تلك المعلومات المتعلقة بإدارة مخاطر الأمن السيبراني. وقد يأخذ هذا الإفصاح شكلين أساسيين؛ الأول الإفصاح ضمن التقارير الأخرى التي تقدمها الشركة في سياق الإفصاح عن مخاطر الأعمال مثل تقرير مجلس الإدارة أو تقرير نتائج الأعمال، أو تقرير الحوكمة والاستدامة، والثاني هو الإفصاح في تقرير مستقل عن إدارة مخاطر الأمن السيبراني.

ثانياً: الحالة التجريبية:

قامت شركة "بنك الحضارة" وهى أحد أكبر البنوك التجارية التي تعمل في مصر بإصدار القوائم المالية، وذلك عن سنة 2023 على النحو التالي:

1- جزء من القوائم المالية عن السنة المالية المنتهية في 2023/12/31:

قائمة المركز المالي في ٢٠٢٣/١٢/٣١ (بالمليون) جنيه		
	٢٠٢٣	٢٠٢٢
نقدية وأرصدة لدى البنك المركزي والبنوك	٢٦,٠٠٠	١٥,٣٩٥
قروض وتسهيلات للبنوك والعملاء	٣٣,٥١٤	٢٩,٣٢٢
استثمارات مالية	١٥,٥٩٨	١٥,٤٦١
اجمالي الأصول	**٧٥,١١٢**	**٦٠,١٧٨**
ودائع العملاء	٦٠,٤٦٣	٤٨,٤١٦
الالتزامات الأخرى	٤,٧٢٤	٣,٠٩٣
اجمالي الالتزامات	**٦٥,١٨٧**	**٥١,٥٠٩**
رأس المال	٥,٠٠٠	٥,٠٠٠
احتياطيات	١,٠٠١	٨٧١
ارباح مرحلة	٣,٩٢٤	٢,٧٩٨
اجمالي حقوق المساهمين	**٩,٩٢٥**	**٨,٦٦٩**
اجمالي الالتزامات وحقوق المساهمين	**٧٥,١١٢**	**٦٠,١٧٨**

قائمة الدخل الشامل عن الفترة المنتهية في ٢٠٢٣/١٢/٣١ القيمة (بالمليون) جنيه		
	٢٠٢٣	٢٠٢٢
عائد القروض والإيرادات المشابهة	٦,٢٧٥	٥,١٥٧
تكلفة الودائع والتكاليف المشابهة	(٢,٤٧٥)	(٢,٢٣٩)
صافى الدخل من العائد	**٣,٨٠٠**	**٢,٩١٨**
إيرادات الأتعاب العمولات	١,٢٨٥	٩١٦
مصروفات الأتعاب والعمولات	(٤٥٨)	(٣٤٤)
صافى الدخل من الأتعاب والعمولات	**٨٢٧**	**٥٧٢**
صافي إيرادات ومصروفات تشغيل أخرى	(١٣٣٢)	(١,٢٧٩)
صافي الدخل قبل الضريبة	**٣,٣٠٥**	**٢,٢١١**
ضريبة الدخل والضريبة المؤجلة	(٨٨٦)	(٦١٩)
صافي الدخل	**(٢,٤١٩)**	**(١,٥٩٢)**
عناصر الدخل الشامل الاخرى	(٧٦)	(٣٦)
اجمالي الدخل الشامل	**٢,٣٤٣**	**١,٥٥٦**

قائمة التدفقات النقدية عن الفترة المنتهية في ٢٠٢٣/١٢/٣١ القيمة (بالمليون) جنيه		
	٢٠٢٣	٢٠٢٢
صافي التدفقات النقدية من الأنشطة التشغيلية	22110	21808
صافي التدفقات النقدية من الأنشطة الاستثمارية	-15762	-25817
صافي التدفقات النقدية من الأنشطة التمويلية	-8475	-5739
صافي التغير في التدفقات النقدية	**-2127**	**-9748**
رصيد النقدية أول الفترة	5560	15308
رصيد النقدية اخر الفترة	**3433**	**5560**

وقد جاء تقرير مراقب الحسابات عن مراجعة القوائم المالية غير معدل.

وقد تضمن تقرير مجلس الإدارة الجزء التالي:

إدارة المخاطر

لدى البنك هيكل قوي لإدارة المخاطر وإطار عمل يضمن توازناً دقيقا بين المخاطر والعائد، يتضمن الآتي:

- مخاطر السيولة: يركز البنك على أهمية الإدارة الحكيمة للسيولة لضمان أعمال مستدامة ومربحة، وكذلك من أجل الحفاظ على ثقة الأسواق المالية. وتوفر عملية مراقبة إدارة المخاطر ما يضمن أن موارد البنك كافية من حيث الكمية والتنوع مما يسمح باستيعاب الزيادات المخطط لها وغير مخططة في متطلبات التمويل بشكل روتيني دون ترك تأثير سلبي مادي على الأرباح أو وضع البنك في السوق.

- مخاطر السوق: يقوم البنك بفصل التعرض لمخاطر السوق إلى محافظ لأغراض المتاجرة وغير أغراض المتاجرة حيث ترجع أسباب مخاطر السوق بشكل أساسى إلى مخاطر أسعار العائد للمراكز المحتفظ بها لغير أغراض المتاجرة ومخاطر أسعار الصرف التي تنشأ نتيجة أنشطة البنك اليومية. ويدير البنك تلك المخاطر من خلال إطار عمل شامل يعكس القبول المحدود لتلك المخاطر. ويفوض مجلس إدارة البنك لجنة إدارة الأصول للرقابة على إدارة مخاطر السوق.
- المخاطر التشغيلية: يتم تعزيز أطر عمل المخاطر التشغيلية باستمرار ودعم في البنية التحتية لاستمرارية الأعمال ومراكز استمرارية العمل بعد الأزمات، ويستمر تحسين جودة البيانات وإعداد التقارير الخاصة بالمؤشرات الرئيسية للمخاطر مع تطور أطر العمل. ويتم الحفاظ على مستويات منخفضة من المخاطر التشغيلية من خلال استخدام أفضل الأطر التطبيقية والالتزام بتعليمات الجهات التنظيمية والتي تتوافق مع استراتيجية البنك بما يعزز الوعى بثقافة إدارة المخاطر التشغيلية بنطاق اوسع بالبنك، مما يعد من أحد سبل الشراكة في رفع كفاءة العمل.
- مخاطر الائتمان: يدير البنك مخاطر الائتمان من خلال إطار عمل من النماذج والسياسات الاجراءات التي تقيس وتسهل إدارة مخاطر الائتمان. بما يضمن الفصل التام للمهام بين ادارة العلاقة الائتمانية مع العملاء ووظيفة تحليل ومراجعة مخاطر الائتمان. ويتم الموافقة على حدود التعرض لمخاطر الائتمان في إطار محدد للسلطات الائتمانية. وتوجد لدى البنك عملية متاكملة تغطي بدء منح الائتمان، والتحقق من صحة التقييم، والتحليلات، والموافقات، ورصد الحدود على مستويات متعددة.
- المخاطر البيئية والاجتماعية: يقوم البنك بدمج الاعتبارات البيئية والاجتماعية في القرارات المتعلقة بالتمويل والعمليات الداخلية بغرض تحقيق البنك لربح هادف من خلال تطبيق مفهوم التمويل المستدام والعمليات المستدامة.

وفي ضوء اطلاعك على التقارير السنوية السابقة من فضلك:

<u>أولاً: بصفتك أحد المستثمرين</u> في الأسهم ومهتم بالاستثمار في أسهم "بنك الحضاره":

1- هل توافق على ان هذه البنك سيكون له أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات المنافسة اعتماداً على ما تقدم من معلومات:

10 9 8 7 6 5 4 3 2 1

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

2- إذا كان سعر اقفال السهم للشركة "بنك الحضارة" في 2022/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2023/12/31 كان يبلغ 112 جنيه فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:

يزيد بصورة كبيرة	يزيد بصورة محدودة	لا يتغير بصورة مؤثرة	ينخفض بصورة محدودة	ينخفض بصورة كبيرة

3- ما هو احتمال استثمارك في أسهم شركة "بنك الحضارة":

أكبر من 75%	أكبر 50% وأقل من75%	محايد	أكبر من25% وأقل من 50%	أقل من 25%

ثانياً: بصفتك أحد عملاء البنك:

4- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة:

1 2 3 4 5 6 7 8 9 10

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

من فضلك لا تقوم بتعديل اجاباتك السابقة في ضوء ما سيرد من بيانات في الجزء اللاحق

المرحلة الثانية من التجربة

حيث تم تقديم الإفصاح عن إدارة مخاطر الأمن السيبراني كما يلي:

المجموعة التجريبية الأولى: من خلال تقرير مجلس الإدارة

يفرض أن تقرير مجلس الإدارة أيضاً تضمن الفقرات التالية:

إدارة المخاطر

لدى البنك هيكل قوي لإدارة المخاطر وإطار عمل يضمن توازناً دقيقا بين المخاطر والعائد، يتضمن الآتي:

- مخاطر السيولة: يركز البنك على أهمية الإدارة الحكيمة للسيولة لضمان أعمال مستدامة ومربحة، وكذلك من أجل الحفاظ على ثقة الأسواق المالية. وتوفر عملية مراقبة إدارة المخاطر ما يضمن أن موارد البنك كافية من

حيث الكمية والتنوع مما يسمح باستيعاب الزيادات المخطط لها وغير مخططة في متطلبات التمويل بشكل روتيني دون ترك تأثير سلبي مادي على الأرباح أو وضع البنك في السوق.

- مخاطر السوق: يقوم البنك بفصل التعرض لمخاطر السوق إلى محافظ لأغراض المتاجرة وغير أغراض المتاجرة حيث ترجع أسباب مخاطر السوق بشكل أساسى إلى مخاطر أسعار العائد للمراكز المحتفظ بها لغير أغراض المتاجرة ومخاطر أسعار الصرف التي تنشأ نتيجة أنشطة البنك اليومية. ويدير البنك تلك المخاطر من خلال إطار عمل شامل يعكس القبول المحدود لتلك المخاطر. ويفوض مجلس إدارة البنك لجنة إدارة الأصول للرقابة على إدارة مخاطر السوق.
- المخاطر التشغيلية: يتم تعزيز أطر عمل المخاطر التشغيلية باستمرار ودعم في البنية التحتية لاستمرارية الأعمال ومراكز استمرارية العمل بعد الأزمات، ويستمر تحسين جودة البيانات وإعداد التقارير الخاصة بالمؤشرات الرئيسية للمخاطر مع تطور أطر العمل. ويتم الحفاظ على مستويات منخفضة من المخاطر التشغيلية من خلال استخدام أفضل الأطر التطبيقية والالتزام بتعليمات الجهات التنظيمية والتي تتوافق مع استراتيجية البنك بما يعزز الوعى بثقافة إدارة المخاطر التشغيلية بنطاق اوسع بالبنك، مما يعد من أحد سبل الشراكة في رفع كفاءة العمل.
- التهديدات الالكترونية: التهديدات العالمية في الفضاء الالكتروني في تزايد مستمر عالميا. وتعتبر مخاطر الفضاء الالكتروني من أهم المخاطر التي تحظى بإهتمام الإدارة العليا في كافة المجالات. ويتكون فريق أمن المعلومات من عدد من الخبراء في مجال الأمن السيبراني في جميع المجالات الأمنية الذين يفكرون وينفذون الضوابط الأمنية في جميع المراحل (قبل وأثناء وبعد) أي حادث أمني للمساعدة في الحماية الفعالة والمراقبة والكشف والتحليل والتحقيق وتقديم توصيات الإصلاح كجزء من مهمتنا الأساسية للأمن السيبراني.
- مخاطر الائتمان: يدير البنك مخاطر الائتمان من خلال إطار عمل من النماذج والسياسات الاجراءات التي تقيس وتسهل إدارة مخاطر الائتمان. بما يضمن الفصل التام للمهام بين ادارة العلاقة الائتمانية مع العملاء ووظيفة تحليل ومراجعة مخاطر الائتمان. ويتم الموافقة على حدود التعرض لمخاطر الائتمان في إطار محدد للسلطات الائتمانية. وتوجد لدى البنك عملية متاكملة تغطي بدء منح الائتمان، والتحقق من صحة التقييم، والتحليلات، والموافقات، ورصد الحدود على مستويات متعددة.
- المخاطر البيئية والاجتماعية: يقوم البنك بدمج الاعتبارات البيئية والاجتماعية في القرارات المتعلقة بالتمويل والعمليات الداخلية بغرض تحقيق البنك لربح هادف من خلال تطبيق مفهوم التمويل المستدام والعمليات المستدامة.

المجموعة التجريبية الثانية: من خلال تقرير منفصل

بفرض أن البنك قدم تقريراً منفصلاً عن إدارة مخاطر الأمن السيبراني للبنك على النحو التالي:

تقرير إدارة مخاطر الأمن السيبراني لبنك الحضارة

السادة مساهمي-عملاء بنك الحضارة:

نظراً لأهمية الأمن السيبراني وحماية خصوصية وحسابات العملاء، فقد التزم البنك بتصميم وتشغيل أنظمة فعالة ومرنة تضمن الأمن السيبراني وتحمي خصوصية العملاء، وفقاً لأحدث المعايير العالمية، والتي مكنت البنك من عدم التعرض لأي مخاطر تهدد أمنه السيبراني أو خصوصية حسابات العملاء للخطر.

تم إعداد هذا التقرير اعتماداً على الإطار الصادر عن المعهد الأمريكي للمحاسبين القانونيين بخصوص التقرير عن إدارة مخاطر الأمن السيبراني.

ويعرض التقرير ملخصاً لأهم السياسات التي اتبعها البنك في هذا الصدد:

1- قام "بنك الحضارة" بتطبيق حوكمة قوية للأمن السيبراني من خلال مركز عمليات أمنية يعمل على مدار 24 ساعة طوال أيام الأسبوع للمراقبة المستمرة والاستجابة للتهديدات.

2- حصل البنك على شهادات في صناعة بطاقات الدفع – معايير أمن البيانات، ISO 22301 لإدارة استمرارية الأعمال، و27001 ISO لإدارة أمن المعلومات، وكذلك ISO27005 لإدارة مخاطر أمن المعلومات. وبالتالي فإن منهجية إدارة مخاطر الأمن السيبراني قد تم تطويرها اعتماداً على الأطر والمعايير المعتمدة دولياً بتلك الجهات وكذا استرشاداً بمعايير الهيئة الوطنية للمعايير والتكنولوجيا الأمريكي NIST، واتساقاً مع الاستراتيجية الوطنية المصرية للأمن السيبراني.

3- من أجل ضمان سرية البيانات وسلامتها وتوافرها مع ضمان استمرارية العمليات التجارية الهامة في جميع الأوقات، يضع بنك الحضارة الاستراتيجيات والضوابط والخطط التي تسهل الإدارة الكافية لجميع التهديدات الأمنية وحوادث تعطل الأعمال. ويتضمن ذلك:

أ- مراقبة دقيقة للتهديدات المحتملة، وتحديد العمليات التجارية الهامة وترتيب أولوياتها، والتخطيط بشكل استباقي لسيناريوهات أسوأ الحالات.

ب- يعمل نظام الأمن السيبراني الخاص ببنك الحضارة على حماية البنك من التهديدات الأمنية المحتملة واضطرابات الأعمال ونقاط الضعف مع الحفاظ على المرونة التنظيمية

أثناء أحداث الأزمات التي قد تهدد صحة وسلامة وأمن الأشخاص (الموظفين أو العملاء) أو قد تؤثر بشدة على خدمات البنك.

ج- تتوافق إستراتيجية الأمن والمرونة الخاصة ببنك الحضارة مع الإستراتيجية والتطلعات الرقمية للبنك، مع البقاء على اطلاع بمشهد التهديدات المتغير باستمرار وتقنيات الهجوم المتطورة.

د- ينصب تركيز بنك الحضارة على ضمان أمن المعلومات، وحماية البيانات، والأمن السيبراني، والتعافي من الكوارث، واستمرارية الأعمال، وإدارة الأزمات.

ه- في عام 2022، قام بنك الحضارة بتحديث جميع سياسات تكنولوجيا المعلومات والأمن السيبراني الخاصة به، بما يتوافق مع ISO 22301– أنظمة إدارة استمرارية الأعمال، ISO 27001– أنظمة إدارة أمن المعلومات، معيار أمن بيانات صناعة بطاقات الدفع (PCI–DSS)، أهداف التحكم بالمعلومات والبيانات ذات الصلة. التقنيات (COBIT)، ولوائح البنك المركزي المصري، وبرنامج SWIFT لأمن العملاء (CSP)، والقوانين واللوائح ذات الصلة.

و- يوضح بنك الحضارة تفانيه في دعم أفضل ممارسات الصناعة والمعايير الدولية من خلال الحفاظ على شهادات PCI وISO. يؤكد التجديد الناجح لهذه الشهادات مؤخرًا في عام 2022 على التزام بنك الحضارة المستمر بتلبية المتطلبات الصارمة لنظام أمن البيانات وإدارتها.

ز- بالإضافة إلى ذلك، أجرى بنك الحضارة جلسات تعريفية حول استمرارية الأعمال وأمن المعلومات للموظفين الجدد وقدم العديد من جلسات التدريب والتوعية للموظفين الحاليين. تركز هذه المبادرات على دمج المرونة في العمليات اليومية وتعزيز الوعي بالامتثال لـ PCI. برنامج شامل للتوعية الأمنية قام بنك الحضارة بتنفيذ برنامج شامل للتوعية الأمنية لتعزيز المعرفة واليقظة لكل من الموظفين والعملاء. يتضمن هذا البرنامج العديد من الحملات الداخلية والخارجية التي أثبتت فعاليتها في زيادة الوعي بين الموظفين وتعزيز دفاعات البنك ضد الهجمات الإلكترونية. علاوة على ذلك، يعطي البرنامج الأولوية لسلامة وأمن العملاء، مما يوفر تجربة أكثر أمانًا عند استخدام القنوات الرقمية للبنك. ويتجلى نجاح هذه المبادرة في تحسين الممارسات الأمنية وانخفاض الحوادث الأمنية، مما يؤدي في نهاية المطاف إلى إضافة قيمة من خلال حماية المعلومات الحساسة وحماية مصالح كل من البنك وعملائه. برنامج تصنيف وحماية البيانات في عام 2022،

أكمل بنك الحضارة بنجاح تنفيذ برنامج تصنيف وحماية البيانات، بهدف حماية بيانات البنك والعملاء. وقد حقق المشروع نجاحًا باهرًا، مما أدى إلى التصنيف المناسب لمختلف أنواع البيانات في البنك. من خلال هذا البرنامج، يضمن بنك الحضارة تطبيق الضوابط المناسبة على كل فئة من فئات البيانات، مما يخفف بشكل فعال المخاطر المرتبطة بانتهاكات البيانات والوصول غير المصرح به.

ح- مركز العمليات الأمنية: بنك الحضارة بتوسيع عمليات مركز العمليات الأمنية (SOC) من 5×8 إلى 24×7، مما يتيح المراقبة المستمرة والاستجابة للتهديدات المحتملة. يعمل مركز عمليات الأمن (SOC) الآن على مدار الساعة، مما يتيح اكتشاف الحوادث الأمنية في الوقت المناسب والتخفيف من آثارها. يسمح هذا التوسع بمراقبة أنظمة وشبكات البنك في الوقت الفعلي، مما يعزز قدرة البنك على تحديد أي مخاطر أمنية ناشئة والاستجابة لها على الفور

وتؤكد الإدارة على أن تلك السياسا والإجراءات كافية لحماية الأمن السيبراني للبنك، وأنها تنفذ بكفاءة وفاعلية عالية، وترتب على ذلك عدم وجود أي اختراقات للبيانات، أو عمليات احتيال خلال السنة محل التقرير.

ثم تم الطلب من المشاركين في المجموعتين بالإجابة على التساؤلات التالية

<u>أولاً: بصفتك أحد المستثمرين:</u>

5- هل ترى أن الإفصاح عن إدارة مخاطر **الأمن السيبراني** ضمن تقرير مجلس الإدارة السابق الإشاره إليه يوفر لك معلومات مفيدة **<u>يمكن الاعتماد</u>** عليها عند اتخاذ قرار الاستثمار: (من فضلك أعطي درجة من 1-10) والتي تمثل مستوى إعتمادك على ما ورد بالتقرير كأحد أهم مدخلات قرارات الاسثمار:

10	9	8	7	6	5	4	3	2	1
○	○	○	○	○	○	○	○	○	○

6- إذا كان سعر اقفال السهم للشركة (أ) في 2016/12/31 يبلغ 109 جنيه وسعر اقفال السهم في 2017/12/31 كان يبلغ 112 جنيه. فإن سعر الاقفال من وجهة نظركم المتوقع في 2024/12/31 أن يتغير كالتالي:

يزيد بصورة كبيرة	يزيد بصورة محدودة	لا يتغير بصورة مؤثرة	ينخفض بصورة محدودة	ينخفض بصورة كبيرة

7- ما هو احتمال استثمارك في أسهم تلك الشركة:

أكبر من 75%	أكبر 50% وأقل من75%	محايد	أكبر من25% وأقل من 50%	أقل من 25%

ثانياً: بصفتك أحد عملاء البنك:

8- هل ترى أن المعلومات عن "إدارة مخاطر الأمن السيبراني" الواردة بتقرير مجلس الإدارة السابق الإشار إليه يوفر لك لك معلومات مفيدة وكافية يمكن الاعتماد عليها عند اتخاذ قرار التعامل مع البنك كأحد عملاءه؟ (من فضلك أعطي درجة من 1-10) والتي يمثل مستوى إعتمادك على التقرير كأحد مدخلات قرارات التعامل مع البنك.

10 9 8 7 6 5 4 3 2 1

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

9- هل توافق على أن هذا البنك سيكون له أولوية أكبر لاستخدام خدماته الالكترونية واختيار استخراج البطاقة الائتمانية والتعامل بها عبر المواقع الالكترونية مقارنة بالبنوك المنافسة التي لم تقدم معلومات حول إدارة مخاطر الأمن السيبرني ضمن تقرير مجلس الإدارة؟ (من فضلك أعطي درجة من 1-10) والتي يمثل مستوى إعتمادك على المعلومات الواردة كأحد مدخلات قرارات التعامل مع البنك.

10 9 8 7 6 5 4 3 2 1

○ ○ ○ ○ ○ ○ ○ ○ ○ ○