دور حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني وأثره في تحسين الأداء المالي: دراسة تجريبية على البنوك المقيدة بالبورصة المصرية

د/ ناريمان إسماعيل أحمد البردونى

المدرس بقسم المحاسبة

كلية التجارة – جامعة القاهرة

nariman.elbardony@foc.cu.edu.eg

ملخص البحث

هدف البحث: اختبار مدى مساهمة حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وأثر ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

منهجية البحث: اعتمد البحث على المنهج الوصفي التحليلي والذي يجمع بين كل من التحليل النظري لأهم الأدبيات المختلفة ذات العلاقة بموضوع البحث، وأيضاً إجراء دراسة تجريبية استهدفت عينة من المحاسبين والمراجعين الداخليين بالبنوك المقيدة بالبورصة المصرية، وقد بلغ حجم عينة الدراسة 105 مفردة بنسبة استجابة 100%. وذلك لاختبار فروض البحث باستخدام مجموعة من الأساليب والاختبارات الإحصائية والتي تتمثل في؛ مقاييس الإحصاء الوصفي، ومعامل الثبات ألفا كرونباخ، واختبار ويلكوكسن لعينة واحدة.

نتائج البحث: أوضحت نتائج الدراسة التجريبية؛ أولاً: مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية. ثانيا: مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية. ثالثا: الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني من المتوقع أن يسهم ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

الأصالة والإضافة العلمية للبحث: تظهر الإضافة العلمية للبحث في محاولة المساهمة في البناء المعرفي لأحد الموضوعات التي أثارت اهتمام الساحة الاقتصادية العالمية، وهو موضوع حوكمة الأمن السيبراني ودورها في الحد من مخاطر الهجمات الإلكترونية بالقطاع المصرفي، فضلا عن دورها المتوقع في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني. وخاصة في ظل الحداثة النسبية للموضوع، وعدم اهتمام أي من الدراسات السابقة ذات الأدلة التطبيقية– في حدود ما اطلعت عليه الباحثة– بالتناول المباشر والتفصيلي لاختبار مدى مساهمة تطبيق حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية. كما يعد هذا البحث استكمالاً للبحوث المرتبطة بأسواق المال ونجاح المؤسسات المالية في استمرارية نشاطها، وبالتالي يمكن للمستثمرين ومديري المؤسسات المالية وغيرهم من أصحاب المصالح الاستفادة من نتائجه في ترشيد قراراتهم المالية والاستثمارية.

الكلمات المفتاحية: حوكمة الأمن السيبراني، مخاطر الهجمات الإلكترونية، الإفصاح عن إدارة مخاطر الأمن السيبراني، الأداء المالي، البنوك المصرية.

[1] تقديم البحث في 2024/9/14 وقبول نشره في 2024/10/20

The Role of Cybersecurity Governance in Activating the Disclosure of Cybersecurity Risk Management and its Impact on Improving Financial Performance: An Experimental Study on Banks Listed on the Egyptian Stock Exchange

Abstract

Research objective: the study aimed to test the extent to which Cybersecurity governance contributes to reducing the risks of cyber attacks as an approach to activate the disclosure of the cybersecurity risk management report, and its impact on improving the financial performance of banks listed on the Egyptian Stock Exchange.

Research methodology: The study relied on the descriptive analytical approach, which combines both theoretical analyses of the most important various literatures related to the research topic, and also conducting an experimental study that targeted a sample of accountants and internal auditors in banks listed on the Egyptian Stock Exchange. The sample size was 105 participants with a response rate of 100%, to test the research hypotheses using a set of statistical methods and tests, which were: descriptive statistics measures, Cronbach's alpha coefficient and the one – sample Wilcoxon signed rank test.

Research results: The results of this research indicate: First, Cybersecurity governance contributes positively and significantly in reducing the risks of cyber attacks in banks listed on the Egyptian Stock Exchange. Second, Cybersecurity governance contributes positively and significantly in activating the disclosure of a cybersecurity risk management report in banks listed on the Egyptian Stock Exchange. Third, the disclosure of cybersecurity risk management report under Cybersecurity governance is expected to improve the financial performance of banks listed on the Egyptian Stock Exchange.

Originality/ value: The scientific addition of this research appears in its attempt to contribute to the cognitive construction of one of the topics that has attracted the interest of the global economic arena, which is the topic of Cybersecurity governance and its role in reducing the risks of cyber attacks in the banking sector, in addition to its expected role in activating the disclosure of the cybersecurity risk management report. Especially, the previous studies that were conducted inside Egypt -Within the limits of what the researcher has seen- didn't care about testing directly and in detail the extent to which cyber governance contributes to reduce the risks of cyber attacks as an approach to activate the disclosure of the cybersecurity risk management report, and its reflection on improving the financial performance of banks listed on the Egyptian Stock Exchange.This research is also represents a continuation to the capital market researches, and thus investors, company managers and other stakeholders can benefit from its findings in rationalizing the financial and investment decisions.

Keywords: Cybersecurity governance, Risks of cyber attacks, Disclosure of cybersecurity risk management, Financial performance, The Egyptian Stock Exchange.

1-المقدمة وطبيعة المشكلة

اعتلى موضوع الأمن السيبراني صدارة اهتمام الساحة الاقتصادية العالمية، وذلك باعتبار أن الهجمات الإلكترونية (السيبرانية) تشكل خامس أكبر التهديدات للاقتصاد العالمي، والتي من المرجح أن تصل تكلفتها إلى نحو 10 تريليون دولار بحلول عام 2025، الأمر الذي يتطلب ضرورة تعزيز ثقافة الأمن السيبراني، ورفع الوعى بمخاطر الهجمات الإلكترونية، وذلك من خلال تفعيل منظومة الأمن السيبراني في مختلف القطاعات، وبصفة خاصة القطاع المصرفي كإحدى الركائز الأساسية للاقتصاد الرقمي الآمن، ولكونه يعد أحد أكثر القطاعات المستهدفة والمعرضة لمخاطر الهجمات الإلكترونية بنسبة 65% مقارنة بالقطاعات الأخرى وفق تقديرات البنك الدولى. وبالتالي لم يعد إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للبنوك بأمرٍ كافٍ، بل تتطلب المعايير العالمية ضرورة تضمين الإستراتيجيات والسياسات الخاصة بتلك البنوك جزء خاص بحوكمة الأمن السيبراني، وذلك لتحديد مخاطر الهجمات الإلكترونية وإدارتها ومراجعتها والإفصاح عنها بانتظام.

ومع تزايد التهديدات والتحديات المستقبلية في مجال الأمن السيبراني، وفي ظل ما تشهده بعض الدول من اختراق ات أمنية للبنى التحتية للاتصالات وتكنولوجيا المعلومات، فقد سارعت الكثير من حكومات دول العالم إلى وضع إستراتيجيات للأمن السيبراني، ومنها الحكومة المصرية والتي شكلت المجلس الأعلى للأمن السيبراني، والذي أسفرت جهوده عن وضع الإستراتيجية الوطنية المصرية للأمن السيبراني، متضمنة عددا من البرامج التي تدعم الأهداف الإستراتيجية للأمن السيبراني لمختلف القطاعات. وفيما يتعلق بالقطاع المصرفي وتدعيم قدرته على التصدي للهجمات الإلكترونية، فقد قام البنك المركزي المصري بإنشاء مركز متخصص لأمن المعلومات، ليكون بمثابة خط الدفاع الأول في مواجهة وكشف التهديدات الإلكترونية وتحذير البنوك منها. وذلك ضمن منظومة متكاملة يتبناها البنك المركزي المصري لتعزيز الأمن السيبراني، والتي تتضمن مراجعة استعدادات البنوك وقدرتها على التصدي للهجمات الإلكترونية، والتأكد من مطابقة أمن المعلومات بالبنوك للمعايير العالمية على مستوى كل من؛ القدرات البشرية، والقواعد والإجراءات الحاكمة، والأجهزة والتقنيات التكنولوجية.

الأمر الذي يضع البنوك المصرية أمام تحدٍ جديد للحفاظ على مركزها التنافسي، ويفرض على رؤسائها ضرورة إدراك أهمية الأمن السيبراني في ظل اقتصاد رقمي محاط بالتهديدات والمخاطر السيبرانية، ويتطلب منهم ضرورة هيكلة الضوابط الأساسية للأمن السيبراني. والتي يأتي على رأسها تبنى إستراتيجية متكاملة للحوكمة السيبرانية، تمكنها من تحديد مخاطر الهجمات الإلكترونية وإدارتها ومراجعتها والإفصاح عنها

بانتظام، وذلك لتعزيز جودة الخدمات الإلكترونية المقدمة للعملاء، وبالتالي زيادة قدرتها التنافسية وتحسين أدائها المالي.

وفي هذا الصدد، اهتمت المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن مخاطر الأمن السيبراني وبرنامج إدارتها، ويأتي في مقدمتها الإرشادات الصادرة عن هيئة الأوراق المالية والبورصات الأمريكية The U.S. Securities and Exchange Commission (SEC) في2011م، والتي تم تحديثها في عام 2018م. كما قام المعهد الأمريكي للمحاسبين القانونيين The American Institute of Certified Public Accountants (AICPA) بوضع إطار للتقرير عن إدارة مخاطر الأمن السيبراني، وذلك لإرشاد منشآت الأعمال فيما يتعلق بتعزيز إفصاحتها المتعلقة بالأمن السيبراني. وقد وجاء ذلك استجابةً لشكاوى المستثمرين وغيرهم من أصحاب المصالح من عدم وجود معلومات كافية، وفي الوقت المناسب عن مخاطر الأمن السيبراني التي تتعرض لها منشآت الأعمال، وجهودها في إدارة تلك المخاطر، ومن ثم عدم قدرتهم على تقييم موقف الأمن السيبراني لديها ومعرفة مدى فعالية برامجها في إدارة تلك مخاطر.

هذا، وقد اتفقت كثير من الدراسات على أهمية إدارة مخاطر الأمن السيبراني والإفصاح عنها لتحسين الأداء المالي للبنوك. حيث أوضحت تلك الدراسات أن هذا النوع من الإفصاح في التقارير المالية للبنوك، يعتبر بمثابة تأكيد على امتثالها للمتطلبات القانونية والتنظيمية المتعلقة بالأمن السيبراني. كما يعمل على إبراز جهود البنك وقدرته على مواجهة الهجمات الإلكترونية، بما يساعد على زيادة شفافية ووضوح التعامل مع البنك، ومن ثم تمكين العملاء وغيرهم من أصحاب المصالح من تقييم قدرة تلك البنوك على التصدي للتهديدات السيبرانية ومعالجتها، وبالتالي تعزيز الثقة بالخدمات المصرفية المقدمة، وهو ما يعمل بدوره على جذب مزيد من العملاء، ومن ثم زيادة المدخرات وارتفاع نسب السيولة لدى البنك، بما يسهم في تحسين أدائه المالي (قاسم ورشوان، 2022؛ أحمد، 2023؛ أبو سمك، 2023؛ Gatzert and Schubert, 2022; Mazumder and Hossain, 2022).

إلا أنه على النقيض مما سبق، يرى بعض الباحثين (Li et al, 2018; Walton et al., 2021; Cheong et al., 2021) أن الإفصاح عن إدارة مخاطر الأمن السيبراني يعد سلاحًا ذا حدين، حيث وإن كان يحقق العديد من المنافع، إلا أنه يثير المخاوف بشأن احتمال وقوع حوادث سيبرانية في المستقبل، وذلك حال استغلال المهاجمين للمعلومات المتعلقة بحوادث الأمن السيبراني المفصح عنها، والإجراءات المضادة التي تتخذها المنشأة لمواجهتها، والبحث عن ثغرات جديدة لمهاجمة تلك المنشآت وتهديد أمنها السيبراني، وبالتالي التأثير بشكل سلبي على أدائها المالي. فضلا عن المخاوف بشأن استغلال المديرين

للسطلة الممنوحة لهم في إخفاء المعلومات والأخبار المتعلقة بحوادث الأمن السيبراني، وذلك لتجنب المخاطر المحتملة المتعلقة بالإفصاح عن تلك المخاطر؛ مما يزيد بدوره من مشكلة عدم تماثل المعلومات. كما يرى البعض الأخر (Goel and Shawky, 2014; Berkman et al., 2018; Tosun, 2021) أن الإفصاح عن مخاطر الأمن السيبراني قد يحمل في طياته نغمة سلبية تنعكس على تقييم المستثمرين لأداء المنشأة، وأن الإعلان عن حدوث هجمات إلكترونية قد يزيد خطر انخفاض العوائد اليومية، ويؤثر سلبًا على أحجام التداول.

ويثير هذا الأمر بدوره التساؤل عن مدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على الأداء المالي وبصفة خاصة في القطاع المصرفي، باعتبار أن البنوك من أكثر منشآت الأعمال استهدافًا بالهجمات الإلكترونية. إذ تتوقع الباحثة وجود تأثير إيجابي لتطبيق ضوابط حوكمة الأمن السيبراني على تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني بالبنوك المصرية، وذلك نظرا لدورها الفعال في دعم وتعزيز الأمن السيبراني لمنشآت الأعمال على نحو مستمر، ومن ثم التغلب على المخاوف المصاحبة لهذا النوع من الإفصاح، بما يسهم في تشجيع منشآت الأعمال بصفة عامة والبنوك المصرية بصفة خاصة على الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وهو ما يمكن أن يؤدي بدوره إلى زيادة قدرتها التنافسية وبالتالي تحسين أدائها المالي.

وتأسيسًا على ما تقدم، وفي ظل تباين الآراء وعدم اهتمام أي من الدراسات السابقة وبصفة خاصة في البيئة المصرية – في حدود ما اطلعت عليه الباحثة – بالتناول المباشر والتفصيلي لاختبار مدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية، **تتلخص مشكلة البحث** في الإجابة عن التساؤلات التالية:

- ما المقصود بالهجمات الإلكترونية، وما هي طبيعة وأشكال المخاطر المرتبطة بها؟
- ما المقصود بالأمن السيبراني وما هي أهدافه وأبعاده؟
- ما المقصود بحوكمة الأمن السيبراني، وما هي ضوابط تطبيقها بالبنوك؟
- هل تسهم حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية، وبالتالي تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وتحسين الأداء المالي؟

2- هدف البحث

في ضوء طبيعة المشكلة، يتمثل الهدف الرئيس للبحث في **دراسة وتحليل مدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في الحد على مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وأثر ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.** وينبثق عن هذا الهدف الرئيس مجموعة من الأهداف الفرعية التالية:

- **الهدف الفرعي الأول:** دراسة وتحليل ماهية الهجمات الإلكترونية من حيث المفهوم، ومخاطر الهجمات الإلكترونية فيما يتعلق بأمن المعلومات، إلى جانب طبيعة وأشكال الهجمات الإلكترونية في القطاع المصرفي.
- **الهدف الفرعي الثاني:** دراسة وتحليل ماهية الأمن السيبراني بالقطاع المصرفي من حيث المفهوم، والأبعاد، والأهداف، ومراحل البناء، وأيضا بعض الجهود العربية في هذا المجال.
- **الهدف الفرعي الثالث:** دراسة وتحليل ماهية حوكمة الأمن السيبراني من حيث المفهوم، والأهداف، والضوابط.
- **الهدف الفرعي الرابع:** دراسة وتحليل ماهية الإفصاح عن إدارة مخاطر الأمن السيبراني، ودوره في تحسين الأداء المالي في ظل تطبيق ضوابط حوكمة الأمن السيبراني بالبنوك.
- **الهدف الفرعي الخامس:** اختبار العلاقات المختلفة بين متغيرات الدراسة، وتقديم دليل تطبيقي بشأن مدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

3- أهمية البحث

في ضوء طبيعة المشكلة وهدف البحث، فإن أهمية البحث تتمثل في كل من الأهمية العلمية والأهمية العملية للبحث، وذلك على النحو التالي:

- **الأهمية العلمية:** وتتمثل في محاولة المساهمة في البناء المعرفي لأحد الموضوعات التي أثارت اهتمام الساحة الاقتصادية العالمية، وهو موضوع حوكمة الأمن السيبراني ودوره في الحد من مخاطر الهجمات الإلكترونية بالقطاع المصرفي، فضلا عن دورها المتوقع في تفعيل الإفصاح عن تقرير إدارة مخاطر

الأمن السيبراني، وخاصة في ظل الحداثة النسبية للموضوع وندرة الدراسات السابقة ذات الصلة بموضوع البحث.

- **الأهمية العملية:** والتي تنبع من واقع عدم اهتمام أي من الدراسات السابقة ذات الأدلة التطبيقية – في حدود ما اطلعت عليه الباحثة – بالتناول المباشر لمدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية. وبالتالي محاولة وضع إطار مرجعي للحوكمة السيبرانية والخروج بمجموعة من النتائج والتوصيات التي يمكن أن تستفيد منها البنوك المصرية في تعزيز الأمن السيبراني للمنتجات والخدمات الإلكترونية المقدمة للعملاء، ومن ثم زيادة قدرتها التنافسية وتحسين أدائها المالي.

4-نطاق البحث

اقتصر البحث على حوكمة الأمن السيبراني كواحدة من الضوابط الرئيسية للأمن السيبراني وعلاقتها بتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على تحسين الأداء المالي، دون غيرها من الضوابط الأخرى التي تخرج عن نطاق هذا البحث. كما اقتصر مجتمع الدراسة التجريبية على البنوك المقيدة بالبورصة المصرية، وذلك خلال العام 2024.

5-منهج البحث

يتمثل منهج البحث في المنهج الوصفي التحليلي والذي يجمع بين كل من التحليل النظري لأهم الأدبيات المختلفة ذات العلاقة بموضوع البحث، وأيضاً الاعتبارات التطبيقية والعملية. ومن ثم يرتكز منهج البحث على محورين أساسيين، هما:

- **المحور الأول:** يتمثل في الدراسة النظرية، والتي تقوم خلالها الباحثة بعرض تأصيل مفاهيمي للمتغيرات التي يتناولها عنوان البحث، بالإضافة إلى عرض وتصنيف وتحليل الدراسات السابقة ذات العلاقة بموضوع البحث، بما يفيد في تحقيق هدف البحث.

- **المحور الثاني:** يتمثل في الدراسة التجريبية، والتي تهدف من خلالها الباحثة إلى اختبار فروض البحث في الواقع العملي. ويشتمل هذا المحور على تحديد مجتمع وعينة الدراسة، وتصميم الدراسة التجريبية، وتوصيف متغيرات الدراسة، واختيار الأساليب الإحصائية الملائمة، ثم ينتهي هذا المحور بعرض ومناقشة نتائج التحليل الإحصائي.

6-تبويب البحث

في ضوء طبيعة مشكلة البحث، وفي سبيل تحقيق أهدافه، سيتم استكماله في الأجزاء التالية:

6-1 الإطار المفاهيمي للبحث

6-2 الدراسات السابقة واشتقاق فروض البحث

6- 3 الدراسة التجريبية

6- 4 خلاصة البحث ونتائجه والتوصيات ومقترحات الأبحاث المستقبلية.

6- 1 الإطار المفاهيمي للبحث

6-1-1 مقدمة

تشهد الساحة الاقتصادية العالمية حراكًا قويًا في مجال تعزيز الأمن السيبراني، وذلك تزامنا مع زيادة وتيرة الهجمات الإلكترونية على منشآت الأعمال، وعلى رأسها البنوك. الأمر الذي ترتب عليه زيادة الاهتمام العالمي باتخاذ العديد من التدابير والإجراءات لتعزيز حوكمة الأمن السيبراني فيما يعرف بالحوكمة السيبرانية، فضلا عن المناداة بضرورة إفصاح منشآت الأعمال عن جهودها في هذا المجال، وذلك بما يضمن تنظيم الفضاء الإلكتروني وحماية منشآت الأعمال بصفة عامة والبنوك بصفة خاصة من التهديدات والمخاطر السيبرانية على كافة المستويات، ولذلك تهدف الباحثة من خلال هذا الجزء إلى دراسة وتحليل ماهية كل من؛ الهجمات الإلكترونية، والأمن السيبراني، وحوكمة الأمن السيبراني، والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني. وذلك كمحاولة لتأطير وتوفير دليل مرجعي لمتطلبات حوكمة الأمن السيبراني للحد من مخاطر الهجمات الإلكترونية، ودورها في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وذلك في ضوء الأطر والإرشادات الصادرة عن المنظمات والهيئات الدولية المعنية بالأمن السيبراني في منشآت الأعمال، وبيان أثر ذلك على تحسين الأداء المالي في البنوك بصفة خاصة.

6-1-2 الهجمات الإلكترونية

تستهدف هذه النقطة البحثية تحديد ماهية الهجمات الإلكترونية من حيث المفهوم، والمخاطر المرتبطة بها وعلاقتها بأمن المعلومات، إلى جانب طبيعة وأشكال الهجمات الإلكترونية في القطاع المصرفي، وذلك على النحو التالي:

6-1-2-1مفهوم الهجمات الإلكترونية

توجد عدة تعريفات لمصطلح الهجمات الإلكترونية حيث تناولته بعض الدراسات من زوايا مختلفة، ومنها دراسة (السمحانى، 2020) والتي عرفت الهجمات الإلكترونية بأنها " المحاولات الضارة والمتعمدة من جانب فرد أو مؤسسة لاختراق نظام المعلومات لدى فرد أو مؤسسة أخرى". كما عرفتها دراسة (إسماعيل، 2020) بأنها " اعتداءات ضارة ومتعمدة يتم تنفيذها عبر الفضاء الإلكتروني من قبل مهاجم (فرد أو منظمة أو دولة)، لاختراق نظام معلومات أو تعطيل شبكة لآخر (فرد أو منظمة أو دولة)، وذلك من خلال نشر برامج ضارة (الفيروسات) تسفر عن أضرار بعيدة المدى، لتحقيق أهداف اقتصادية أو اجتماعية أو سياسية، وغالبا ما يستهدف الهجوم الشركات والمنظمات التجارية والوطنية.

وعرفتها دراسة (Bendovschi, 2015) بأنها " مجموعة من العمليات التي تستهدف التسلل إلى مواقع إلكترونية غير مصرح بالدخول إليها، وذلك لتعطيل أو إتلاف أو الاستحواذ على البيانات الموجودة عليها". كما عرفتها دراسة (Roscini, 2010) بأنها " أي تصرف إلكتروني دفاعي كان أو هجومى يتوقع منه إلحاق أضرار مادية أو تدمير للهدف الذي يتم مهاجمته ". في حين عرفها المركز القومي الأمريكي للبحوث The US National Research Council في 2009 " بأنها الإجراءات المتعمدة لتغيير أو تعطيل أو إتلاف أو خداع أو تدمير أنظمة وشبكات المعلومات" (Hathaway et al., 2012).

مما سبق يتضح للباحثة أنه على الرغم من تعدد التعريفات السابقة لمصطلح الهجمات الإلكترونية، إلا أن مضمون هذه التعريفات جاء متقاربًا في المعنى بشكل كبير، وهو تهديد أمن المعلومات الرقمية للأفراد أو منشآت الأعمال على اختلاف أنواعها، وبالتالي يمكن للباحثة تعريف الهجمات الإلكترونية بأنها " عمليات تستهدف اختراق نظم المعلومات الرقمية الخاصة بالأفراد أو المؤسسات بهدف سرقتها أو التعديل عليها أو إتلافها لأغراض إجرامية مختلفة، وذلك بالاعتماد على البرامج والتقنيات الحديثة في مجال تكنولوجيا المعلومات".

6-1-2-2 المخاطر المرتبطة بالهجمات الإلكترونية وعلاقتها بأمن المعلومات

يشير مصطلح أمن المعلومات إلى حماية كافة المعلومات، سواء كانت رقمية أو غير رقمية من أي استخدام غير مصرح به. وذلك من خلال توفير مستوى مناسب من سرية المعلومات، إلى جانب التأكيد على سلامة ودقة المعلومات وتأمينها ضد حدوث أي تغييرات غير سليمة، وأيضا ضمان قابلية المعلومات للتداول والوصول إليها بسهولة وفي الوقت المناسب (أحمد، 2021؛ العلوان، 2018؛ Solms and Solms, 2018). مما يشير إلى وجود ثلاثة أبعاد رئيسية لأمن المعلومات وهى؛ السرية والنزاهة واستمرارية الأداء (البغدادى 2021).

وفي ذات السياق، أوضحت دراستي (البغدادى، 2021 ;Hartmann and Carmenate, 2021) أن الهجمات الإلكترونية تؤثر فى الجوانب الرئيسية لأمن المعلومات بمنشآت الأعمال، وذلك نظرا لما تحدثه من مخاطر على سرية ونزاهة واستمرارية الأداء، والتي يمكن إيضاحها على النحو التالي:

- **مخاطر تتعلق بالسرية:** والتي تشير إلى الخسائر المحتملة عندما تنجح الهجمات الإلكترونية في اختراق نظام المعلومات الخاص بالمنشأة، والكشف عن البيانات الخاصة بها وبعملائها إلى طرف ثالث غير مصرح له بالوصول إليها.
- **مخاطر تتعلق بالنزاهة:** والتي تشير إلى الخسائر المحتملة عندما تنجح الهجمات الإلكترونية في إساءة استخدام أنظمة المعلومات الخاصة بمنشآت الأعمال، وتنفيذ جرائم الاحتيال من خلالها.
- **مخاطر تتعلق باستمرارية الأداء:** والتي تشير إلى الخسائر المحتملة عندما تنجح الهجمات الإلكترونية في التأثير على توافر البيانات وتعطيل أو تدمير نظام المعلومات الخاص بالمنشأة.

وفي هذا الصدد، أوضحت الإستراتيجية الوطنية المصرية للأمن السيبراني (2017 – 2021) أن خطورة الهجمات الإلكترونية ترجع إلى ثلاثة عناصر رئيسية يمكن إيضاحها على النحو التالي: (الإستراتيجية الوطنية للأمن السيبراني 2018)

- **استنادها إلى تقنيات متقدمة ومتطورة:** والتي غالبا ما تكون حكرا على دول معدودة وشركات كبرى، وكثير منها تكون تقنيات سرية وغير متاحة للتصدير، وتحتوي النسخ المتاحة منها للتصدير على ثغرات تجعلها مصدرا لتهديدات إضافية.
- **سهولة وسرعة انتشارها:** حيث أن شن الهجمات الإلكترونية ونشر البرامج الخبيثة (الفيروسات) يمكن أن يتم بسرعة وبسهولة فائقة عبر الحدود ومن أي مكان، وذلك في ظل انتشار واتساع نطاق استخدام شبكات الإتصالات وتكنولوجيا المعلومات، مع صعوبة تعقب مصدر تلك التهديدات في الوقت المناسب لتداركها والتغلب عليها.
- **اتساع نطاق تأثيرها:** وذلك سواء من حيث التأثير المباشر أو غير المباشر على البنى التحتية، وما قد يتبعه من أضرار أو خسائر فادحة، وكذلك من حيث إمكانية الإضرار بمصالح الجهات العامة والخاصة، والتأثير على جموع كبيرة من المواطنين بصورة مفاجئة، وفي وقت قصير وعن بعد.

6-1-2-3 طبيعة وأشكال الهجمات الإلكترونية في القطاع المصرفي

يعتبر القطاع المصرفي من أكثر القطاعات التى تتعرض لمخاطر الهجمات الإلكترونية بنسبة 65% مقارنة بالقطاعات الأخرى، وذلك وفقا لتقديرات البنك الدولي (إسماعيل، 2019)، ومن أبرز أشكال هذه الهجمات في هذا القطاع كما أوضحتها دراسات (البغدادى، 2021؛ أبو الخير، 2022؛ Antonic, 2018; Skinner, 2019; Bukht et al., 2020) ما يلي:

أ) هجمات تخريب البنية التحتية للبنك

حيث تشمل البنية التحتية للقطاع المالي أنظمة تسوية المدفوعات، وودائع الأوراق المالية المركزية، ومنصات التداول والمواقع الرسمية الإلكترونية للبنوك وغيرها، والتي تعتبر نقطة الضعف لتحقيق الأمن السيبراني في هذا القطاع. وذلك نظرا لتركز المخاطر مع عدم وجود بدائل، الأمر الذي يترتب عليه حدوث اضطرابات كبيرة في سير العمل بالقطاع المالي وفقد ثقة العملاء في البنوك، وذلك حال تعطل سير عمل البنية التحتية للقطاع ذاته، أو لمجموعة من المؤسسات المالية الرئيسية بالقطاع.

فعلى سبيل المثال لا الحصر؛ حدث في عام 2014 أن تعرض بنك First Investment Bank (FIB) وهو ثالث أكبر البنوك البلغارية لأزمة مالية نتيجة عمليات السحب غير الاعتيادية للمودعين، وجاء ذلك بسبب تعرض البنك لهجوم سيبراني استهدف إرسال رسائل بريد إلكتروني مخادعة تفيد بمعاناة البنك من أزمة سيولة. مما دفع المودعين للاصطفاف أمام فروع البنك مطالبين بسحب أموالهم، الأمر الذي كاد أن ينتهي بانهيار البنك لولا أن تدخلت السلطات البلغارية لإنقاذ الموقف. وفي مارس 2022 أعلن البنك المركزي التونسي تعرضه لهجمة سيبرانية أدت إلى حدوث بعض الاضطرابات على مستوى مجموعة من الأنشطة، ومن بينها الموقع الإلكتروني الرسمي للبنك، إلا أنه قام بالتعاون مع الوكالة الوطنية للسلامة المعلوماتية بتدارك الأمر سريعا والسيطرة على الوضع، وأكد البنك على سلامة كافة المعطيات الخاصة بالنظام المعلوماتي الخاص به.

ب) هجمات استغلال الثغرات

وتسمى أيضا بالهجوم دون انتظار Zero Day Attack ، وهذه النوعية من الهجمات تستهدف نقاط الضعف في البرمجيات وثغراتها الأمنية، وغالبا ما يتم استغلال هذه الثغرات من قبل المهاجمين قبل أن تكتشف الجهات المطورة برامج تصحيحية تعمل على مواجهتها.

ج) هجمات اختراق البيانات الخاصة

حيث تستهدف هذه النوعية من الهجمات سرقة الهوية الرقمية والبيانات الخاصة بعملاء القطاع المالي واستغلالها في الكثير من العمليات الإجرامية. وقد تعرض القطاع المالي في الكثير من دول العالم سواء النامية أو الكبرى للكثير من حوادث اختراق البيانات وسرقتها، فعلى سبيل المثال لا الحصر؛ تعرضت البنوك بالولايات المتحدة الأمريكية لسرقة البيانات الخاصة بأكثر من 147 مليون عميل خلال الفترة من عام 2018 إلى 2020، واختراق أكثر من 260 مليون سجل؛ مما أسفر عن خسائر مالية قدرها 41 مليار دولار خلال تلك الفترة.

د) هجمات استهداف الهواتف الذكية

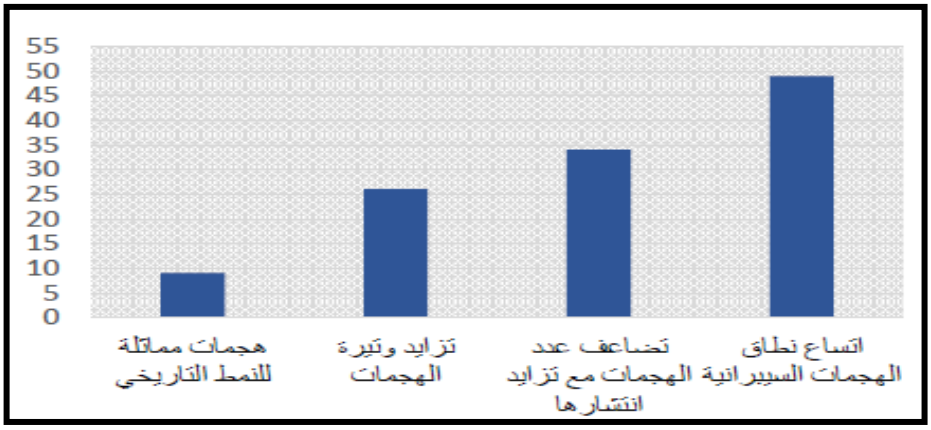
حيث تستهدف هذه الهجمات اختراق الحسابات البنكية للعملاء من خلال التطبيقات البنكية الموجودة على هواتفهم الذكية، وترجع خطورة هذه النوعية من الهجمات إلى أن غالبية مستخدمي الهواتف الذكية، ليس لديهم المعرفة الكافية بالثغرات الأمنية لهذه الهواتف. الأمر الذي يستغله المهاجمون بتوجيه عملاء البنوك نحو تحميل تطبيقات تقع تحت سيطرتهم، وتمكنهم من الحصول على البيانات البنكية الخاصة بهم، أو إصابة النظام الإلكتروني للبنك بالفيروسات التي تعطل عمل النظام بالكامل أو بعض أجزائه.

هـ) هجمات حجب الخدمة

وتستهدف هذه النوعية من الهجمات إغراق مواقع المؤسسات المالية بسيل من البيانات غير الضرورية وذلك لإرباكها وإرباك مستخدميها، حيث ترسل إليها إشارات وطلبات من أجهزة مصابة ببرامج خبيثة (فيروسات) تسمى Attacks DDos والتي يتحكم بها المهاجمون. مما يسبب بطء في الخدمات الإلكترونية للمؤسسة المالية، ويصعب وصول العملاء إليها، وتصبح المؤسسات المالية في ظل هذه النوعية من الهجمات مطالبة بدفع مبالغ معينة للمهاجمين لإنهاء الهجوم عليها.

هذا، وتوضح تقديرات صندوق النقد الدولي للتكلفة الناتجة عن الهجمات الإلكترونية في القطاعات المالية من واقع الخسائر المحققة جراء هجمات فعلية في 50 دولة حول العالم، أن متوسط الخسائر السنوية المحتملة من الهجمات الإلكترونية قد يكون كبيرا بما يقدر بنحو 9% سنويا من صافي دخل البنوك على الصعيد العالمي. وذلك بما يعادل 100 مليار دولار في حال تشابهت هذه الهجمات مع مثيلاتها السابقة، ووفقا للسيناريو شديد الخطورة –حيث يكون تواتر الهجمات الإلكترونية أعلى مرتين مقارنة بمثيلاتها المسجلة في الماضي مع انتشار أكبر للخسائر – يمكن أن تصل تكلفة الخسائر إلى ما يتراوح ما بين 270 إلى 350 مليار دولار سنويا. ووفقا للسيناريو الأسوأ قد تصل التكلفة السنوية المحتملة إلى

50% من صافي دخل البنوك على مستوى العالم، حال اتساع نطاق انتشار الهجمات الإلكترونية في هذا القطاع (Lagarde, 2018)، وذلك كما يتضح من الشكل رقم (1) التالي:



شكل 1: تكلفة الخسائر المحتملة للهجمات الإلكترونية في قطاع الخدمات المالية (كنسبة من صافي الدخل السنوى)

المصدر: (Lagarde 2018)

وفي هذا الصدد، أوضح أيضا البنك الدولي أن نسبة العملاء الذين عانوا من الهجمات الإلكترونية خلال عام 2020 على المستوى العالمي بلغت 72% تقريبا بزيادة قدرها 231% مقارنة بعام 2019، واعترافًا بخطور التهديدات الناجمة عن مخاطر الهجمات الإلكترونية ومدى أهمية تعزيز قدرة الأجهزة المصرفية على تحمل هذه المخاطر والتحوط منها، فقد اتخذت السلطات الرقابية على الصعيد العالمي خطوات تنظيمية وإشرافية لتجنب أثر مخاطر الهجمات الإلكترونية على القطاع المصرفي (إسماعيل 2019؛ World Bank, 2018, 2021). وسارعت المصارف المركزية العربية بإصدار التعليمات التي تحث فيها البنوك على ضرورة وضع الضوابط الأساسية لتعزيز ممارسات الأمن السيبراني للحد من مخاطر الهجمات الإلكترونية وهو ما سوف تتناوله الباحثة في النقطة البحثية التالية.

6-1-3 الأمن السيبراني

تستهدف هذه النقطة البحثية تحديد ماهية الأمن السيبراني من حيث المفهوم، والأبعاد، والأهداف، ومراحل بناء نظام الأمن السيبراني، وأيضا بعض الجهود العربية في هذا المجال، وذلك على النحو التالي:

6-1-3-1 مفهوم الأمن السيبراني

على الرغم من أهمية مفهوم الأمن السيبراني وما أثاره من جدل ونقاش عالمي، إلا أنه لا يوجد تعريف عام متفق عليه لهذا المفهوم، ولعل ذلك مرجعه أنه يشمل أمورا كثيرة لجهات مختلفة، وإن كانت جميعها تدور في نطاق حماية أمن المعلومات الرقمية (Solms and Solms, 2018)، حيث عرفته المنظمة الدولية للمعايير (ISO) بأنه " الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني" (ISO/IEC 27032:2012). وعرفته دراسة (Alina et al., 2017) بأنه " النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانية الحد من الخسائر والأضرار الناتجة عن تحقق المخاطر والتهديدات الإلكترونية، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن في حالة تحقق هذه المخاطر، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة".

كما عرفته دراسة (Potter and Vickers, 2015) بأنه " ممارسة الدفاع عن أجهزة الحاسب الآلي والخوادم والأجهزة المحمولة والشبكات والبيانات من الهجمات الضارة". في حين عرفته دراسة (السمحانى، 2021) بأنه " جميع الإجراءات والتدابير والتقنيات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به". وأيضا عرفته دراسة (Canelon et al., 2020) بأنه "مجموعة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية أجهزة الحاسب الآلي والشبكات والبيانات من الاختراقات أو التلف أو التغيير أو تعطيل الوصول إليها".

ومما سبق يتضح أن الأمن السيبراني يعتبر مفهوم متعدد الأبعاد وله أهميه كبيرة في مختلف قطاعات الأعمال وليس فقط في القطاع المصرفي، ويمكن للباحثة تعريف الأمن السيبراني بأنه " عملية مستمرة لتأمين الأنظمة المتصلة بشبكة الإنترنت متضمنة الأجهزة والبرامج والبيانات من الهجمات الإلكترونية، والتعافي منها حال حدوثها، وذلك على نحو يضمن الحفاظ على سرية البيانات وسلامتها وتوافرها ".

6-1-3-2 أبعاد الأمن السيبراني

أوضحت الإستراتيجية الوطنية المصرية للأمن السيبراني لعام 2018، وأيضا العديد من الدراسات (البغدادى، 2021؛ خشبة وآخرون،2021؛ Akinbowale et al., 2020) أن مفهوم الأمن السيبراني يتداخل مع العديد من الأبعاد، ويمكن إيضاح أهم هذه الأبعاد على النحو التالي:

أ) **البعد الاقتصادي:** ويتمثل في حماية منشآت الأعمال وعلى مستوى كافة القطاعات، وفي مقدمتها القطاع المالي من مخاطر الهجمات الإلكترونية وغيرها من التهديدات السيبرانية، بما يضمن الحفاظ

على سرية البيانات وسلامتها وتوافرها. وذلك من خلال هيكلة الضوابط الأساسية للأمن السيبراني وتنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، للحد من مخاطر الهجمات الإلكترونية وإدارتها ومراجعتها والإبلاغ عنها بانتظام.

ب) **البعد الإجتماعي:** ويتمثل في حماية المجتمع من مخاطر الهجمات الإلكترونية وغيرها من التهديدات السيبرانية، من خلال وضع وتنفيذ خطط وحملات للتوعية المجتمعية بأهمية الأمن السيبراني، والفرص والمزايا التي تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات، وإطلاق برامج حماية الأطفال والنشء على الإنترنت.

ج) **البعد القانوني:** ويتمثل في ضرورة وجود إطار تشريعي ملائم للأمن السيبراني لمكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية وأمن المعلومات، وذلك بمشاركة من الأطراف المعنيين وذوى الخبرة في مختلف القطاعات، مع الاسترشاد بالخبرات والتجارب الدولية ذات الصلة.

د) **البعد السياسي:** ويتمثل في إنشاء منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، ونظم وقواعد البيانات والمعلومات القومية، وبوابات الخدمات الحكومية والمواقع الحكومية على الإنترنت، وذلك بإعداد وتفعيل ما يعرف بفرق الاستعداد والاستجابة لطوارئ الحاسبات والشبكات في القطاعات الحيوية على المستوى الوطني.

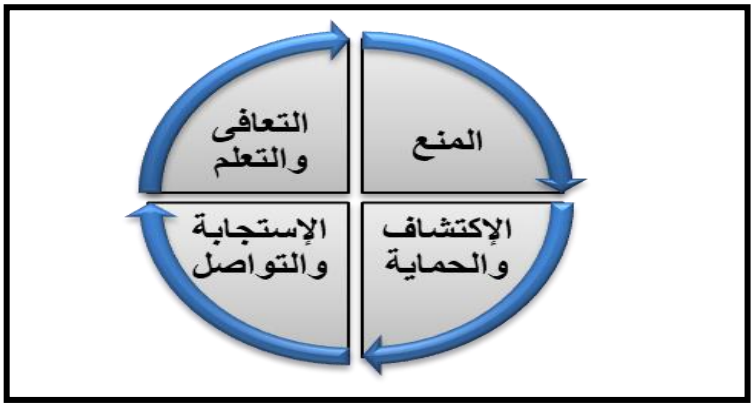
6-1-3-3 أهداف الأمن السيبراني

أوضحت العديد من الدراسات(Yusif and Baig, 2021; Bukht et al., 2021, Maleh et al., 2021; Stanikzai and Shah, 2021; Solms and Solms, 2018) أن للأمن السيبراني الكثير من الأهداف، ولعل من أهم هذه الأهداف ما يلي:

- تعزيز حماية أنظمة تكنولوجيا المعلومات بما تتضمنه من أجهزة وشبكات وبرمجيات وقواعد بيانات، واستكشاف نقاط الضعف والثغرات في هذه الأنظمة ومعالجتها.
- التصدي للهجمات الإلكترونية التي تستهدف الأجهزة الحكومية ومنشآت الأعمال على اختلاف أنواعها، وعلى مستوى كافة القطاعات.
- وضع خطة للتعافي من آثار الهجمات الإلكترونية وضمان استمرار سير العمل.
- توفير بيئة عمل سيبرانية آمنة لإجراء المعاملات المالية وغير المالية في ظل التوجه العالمي نحو التحول الرقمي ودمج التكنولوجيا الرقمية في جميع مجالات الأعمال.

- توفير التدريب اللازم للموظفين فيما يتعلق بكيفية حماية أنظمة تكنولوجيا المعلومات من أي اختراقات أو استخدامات غير مصرح بها، وذلك في مختلف القطاعات، وعلى كافة المستويات.
- تعزيز حماية المجتمع من الجرائم الإلكترونية على اختلاف أنواعها، والتي يتم ارتكابها من خلال شبكات وتقنيات الإنترنت.

وفي هذا الصدد، أوضح المعيار (ISO/IEC 27032:2012) المتعلق بالأمن السيبراني في منظمات الأعمال والصادر عن المنظمة الدولية للمعايير (ISO)، أن إطار عمل الأمن السيبراني يرتكز على أربعة مجالات رئيسية، والتي تعكس أهداف ومدى أهمية وجود نظام للأمن السيبراني بمنظمات الأعمال وعلى رأسها البنوك، ويمكن إيضاحها من خلال الشكل رقم (2) التالي:



شكل 2: إطار عمل الأمن السيبراني

المصدر: (إعداد الباحثة إستنادا إلى المعيار ISO/IEC 27032:2012)

هذا، ويتضح من الشكل رقم (2) السابق أن إطار عمل الأمن السيبراني يرتكز على أربعة مجالات رئيسة يمكن إيضاحها على النحو التالي (ISO/IEC 27032:2012) :

أ) **المنع:** وذلك من خلال تنفيذ التدابير والضوابط التي تمنع، وتحد من الهجمات الإلكترونية وغيرها من تهديدات الأمن السيبراني.

ب) **الاكتشاف والحماية:** وذلك من خلال تطبيق ضوابط إدارة الأمن السيبراني، والمراقبة المستمرة للأحداث الأمنية، بما يساعد في الاكتشاف المبكر للهجمات الإلكترونية وغيرها من التهديدات السيبرانية وتوفير الحماية اللازمة منها.

ج) **الاستجابة والتواصل:** وذلك من خلال تنفيذ خطط الطوارئ واتخاذ الإجراءات اللازمة للتصدي للهجمات الإلكترونية بما يضمن الحفاظ على سرية البيانات وسلامتها وتوافرها، وأيضا توفير الإبلاغ المناسب عن تلك الهجمات والجهود المبذولة في هذا المجال.

د) **التعافي والتعلم:** وذلك من خلال تنفيذ إجراءات استعادة أنظمة تكنولوجيا المعلومات والخدمات المتعلقة بها إلى ما كانت عليه قبل حدوث التهديدات والهجمات الإلكترونية، واتخاذ الإجراءات التصحيحية المناسبة لتقليل احتمالات حدوث مثل هذه الحوادث مجددا.

6-1-3-4 مراحل بناء نظام الأمن السيبراني

قدم المعيار الدولى (ISO/IEC 27032) الصادر عن المنظمة الدولية للمعايير (ISO) مجموعة من الإرشادات التوجيهية التي يمكن أن تستعين بها منشآت الأعمال في عملية بناء نظام للأمن السيبراني، وفي ضوء تلك الإرشادات تمر هذه العملية بأربعة مراحل رئيسية يمكن إيجازها على النحو التالي (ISO/IEC 27032:2012):

- **المرحلة الأولى: فهم المنظمة**

وذلك من حيث طبيعة المنتجات أو الخدمات التي يتم تقديمها للعملاء، ونوعية أنشطة العمليات التي تقوم بها والوظائف المختلفة داخل المنشأة، وأيضا طبيعة البيئة التي تعمل بها وما يرتبط بها من تشريعات ومتطلبات تنظيمية.

- **المرحلة الثانية: تحليل المخاطر**

وذلك من خلال تحديد التهديدات البيئية الداخلية والخارجية، سواء كانت طبيعية أو تقنية أو غير ذلك، والتي يمكن أن يكون لها تأثيرات سلبية على المنشأة، مع وضع الضوابط اللازمة لمنع أو تقليل الخسائر.

- **المرحلة الثالثة: خطة الأمن السيبراني**

في هذه المرحلة يتم هيكلة الضوابط الرئيسية لتحقيق الأمن السيبراني متضمنة سياسات وإستراتيجيات الأمن السيبراني، وتحديد الأدوار والمسؤوليات والضوابط التقنية المختلفة، وذلك على نحو يضمن الحد من مخاطر الهجمات الإلكترونية وغيرها من التهديدات السيبرانية.

- المرحلة الرابعة: التنفيذ

وتستهدف هذه المرحلة تنفيذ ومتابعة الضوابط الرئيسية للأمن السيبراني التي تم تحديدها في المرحلة السابقة، والتأكيد على ضرورة الالتزام بالتنفيذ واستباقية اتخاذ التدابير والإجراءات الأمنية اللازمة مع وضع أسس لتقييم عملية التنفيذ.

6-1-3-5 بعض الجهود العربية في مجال دعم الأمن السيبراني

تبذل الدول العربية كل ما في وسعها للحاق بالركب العالمي في مجال تطوير الأمن السيبراني، وفي هذا الصدد عقدت المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، والمكتب الإقليمي العربي للاتحاد الدولي للاتصالات في شهر نوفمبر 2017 فعالية " الأمن السيبراني في المنطقة العربية "، والتي تضمنت اللقاء الثاني للتجارب الإدارية الناجحة في مجال أمن المعلومات، والمنتدى الإقليمي حول الأمن السيبراني في عصر التكنولوجيا الناشئة، وهدفت هذه الفعالية إلي التعريف بالجهود الإدارية الناجحة في مجال الأمن السيبراني، وذلك من أجل تعميمها ونشرها والاستفادة منها في الدول العربية (أبو زيد، 2019)، ومن من أبرز هذه الجهود – على سبيل المثال لا الحصر – ما يلي:

أ) جهود جمهورية مصر العربية

حيث نصت المادة 31 من الدستور المصري (يناير 2014) على أن " أمن الفضاء المعلوماتي جزء أساسي من منظومة الأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون ". وفي إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبراني والمجتمع الرقمي، ولرصد ومجابهة المخاطر والتهديدات السيبرانية المتزايدة، تم تأسيس المجلس الأعلى للأمن السيبراني والتابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات.

وقد أطلق المجلس الأعلى للأمن السيبراني الإستراتيجية الوطنية للأمن السيبراني (2017– 2021)، والتي تهدف إلى تأمين البنى التحتية للاتصالات والمعلومات على نحو متكامل لتوفير بيئة عمل آمنة لمختلف القطاعات، لتقديم الخدمات الإلكترونية بشكل متكامل (الإستراتيجية الوطنية المصرية للأمن السيبراني 2018). وقام البنك المركزي المصري في إطار تعزيز الأمن السيبراني بالبنوك والمؤسسات المصرفية، وتدعيم قدرتها على التصدي للهجمات الإلكترونية بإنشاء مركز متكامل لأمن المعلومات، يساعد على التنبؤ بالهجمات الإلكترونية قبل وقوعها وتحذير البنوك منها، ومراجعة استعدادات البنوك وقدرتها على التصدي للهجمات الإلكترونية، والتأكد من مطابقة أمن المعلومات بالبنوك للمعايير العالمية

علـى مسـتوى 3 محـددات رئيسـية وهـي؛ الإمكانيـات البشـرية، والقواعـد والإجـراءات الحاكمـة، والأجهـزة والتقنيات التكنولوجية المتوافرة. هذا وقد احتلت مصر خلال عام 2020م المركز 23 عالميًا والرابع عربيًا في المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات (ITU) والذي يضم 182 دولة (طارق وآخرون، 2021؛ ITU 2020).

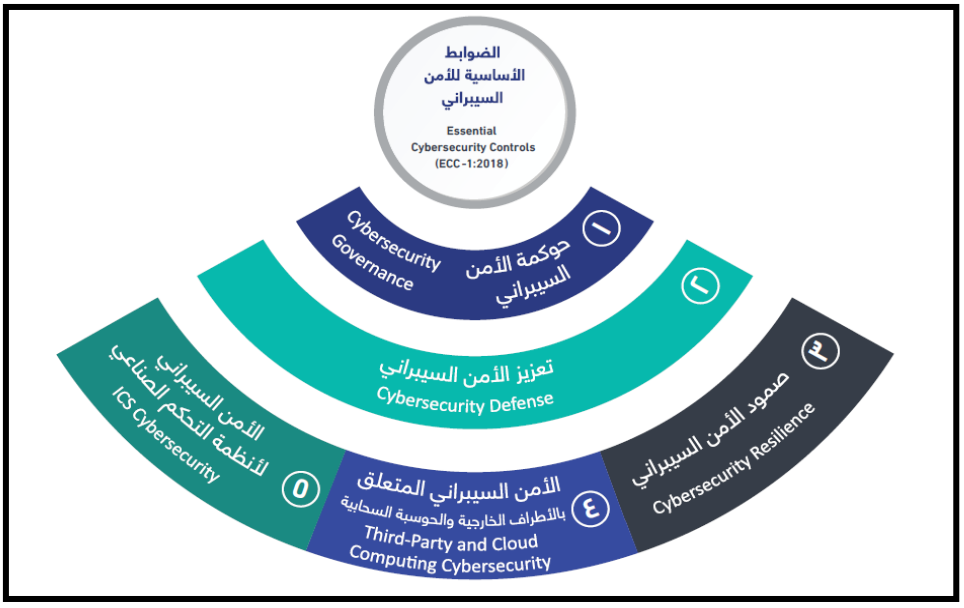
ب) جهود دولة الإمارات العربية المتحدة

احتلت دولـة الإمـارات العربيـة المتحدة خـلال عـام 2020م المركـز الخـامس عالميـا والثـاني عربيًـا فـي المؤشر العالمي للأمن السيبراني GCI (ITU 2020)، وتعد من أوائل الدول العربية التي طبقت نظام الحكومة الإلكترونية الذكية، والقائمة بشكل شبه كامل على تقنيات العالم الرقمي، وهو ما دعاها إلى إطلاق الإستراتيجية الوطنية للأمن السيبراني. والتي تهدف إلى إنشاء بنية تحتية إلكترونية آمنة وقوية للمواطنين، وذلك من خلال تشجيع الابتكار الرقمي، وريادة الأعمال في مجال الأمن السيبراني، وتمكين المؤسسات العامة والخاصة من حماية نفسها من الهجمات الإلكترونية، وكذلك حماية أصول البنية التحتية الهامة، وتكوين قوة عاملة ذات مستوى عالمي للأمن السيبراني في الإمارات العربية المتحدة، وقد صدر القانون رقم 11 لسنة 2014 بشأن إنشاء مركز دبي للأمن الإلكتروني ، والذي يعد مركزا دوليا ذو ريادة تكنولوجية، وتقوم إستراتيجيته على التوعية الأمنية الإلكترونية التي ترمي إلى بناء مجتمع معلوماتي آمن، وأكثر إدراكا لمخاطر الأمن السيبراني (نصار، 2021).

كما نفذت دولـة الإمـارات ممثلـة بهيئـة تنظيم الاتصـالات والحكومـة الرقميـة شبكة اتحاديـة معززة ببنيـة تحتية مشتركة (FedNet) تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتوفر الشبكة بيئة أمن متعددة الطبقات تضمن أعلى مستويات الأمان في البنية التحتية اعتماداً على الترميز متعدد البروتوكولات (MPLS)، وتتيح ربطاً آمناً بالإنترنت لكافة الجهات الحكومية الاتحادية عبر مزود مزدوج لخدمة الإنترنت، ما يسمح بتحقيق إنتاجية أعلى، كما توفر هذه الخدمة اتصالاً موحداً بالإنترنت في الجهات الاتحادية، مما يقلل إمكانية التعرض لهجمات الدخلاء عن طريق الحد من الثغرات. فضـلا عـن إطـلاق مبـادرة (النـبض السـيبراني) وهـي مبـادرة وطنيـة شـاملة تهـدف إلـى نشـر ثقافـة الأمـن السيبراني، وتعزيز مشاركة جميع أفراد المجتمع ورفع وعيهم لأي نشاطات إلكترونية مشبوهة قد تضر بهم، وتمكينهم من استخدام ابتكارات التكنولوجيا الرقمية في بيئةٍ أقل تهديدًا (موقع البوابة الإلكترونية لدولة الإمارات، 2022).

ج) جهود المملكة العربية السعودية

حققت المملكة العربية السعودية قفزة نوعية هامة في عام 2020م باحتلالها المركز الثاني عالميًا والأول عربيًا في المؤشر العالمي للأمن السيبراني GCI وذلك مقابل المركز 46 عالميا على نفس المؤشر في عام 2017م (خشبة وآخرون، 2021 ؛ITU 2021)، فعلى الجانب التشريعي قامت المملكة العربية السعودية بسن القوانين والتشريعات الملائمة لتعزيز الأمن السيبراني ومن أبرزها قانون الجرائم الإلكترونية عام 2017م، وقانون التجارة الإلكترونية عام 2018م (العلوان، 2018؛ خشبة وآخرون، 2021). وعلى الجانب التنظيمي قامت المملكة بتأسيس الهيئة الوطنية للأمن السيبراني في أكتوبر 2017م، والتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – 1 : 2018) وذلك بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني صادرة عن عدة جهات ومنظمات محلية ودولية، إلى جانب دراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، والإطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها وتحليل ما تم رصده من حوادث وهجمات إلكترونية على مستوى الجهات الحكومية وغيرها (الهيئة الوطنية للأمن السيبراني – المملكة العربية السعودية 2018)، ويمكن إيضاح هذه الضوابط من خلال الشكل رقم (3) التالي:



شكل 3: الضوابط الأساسية للأمن السيبراني

المصدر: (الهيئة الوطنية للأمن السيبراني – المملكة العربية السعودية 2018)

هذا، وكما يتضح من الشكل رقم (3) السابق أن حوكمة الأمن السيبراني تأتى على رأس الضوابط الرئيسية للأمن السيبراني، الأمر الذي يستلزم ضرورة دراسة وتحليل ماهية حوكمة الأمن السيبراني كآلية للحد من مخاطر الهجمات الإلكترونية بمنشآت الأعمال، وعلى رأسها البنوك. وهو ما سوف تتناوله الباحثة في النقطة البحثية التالية.

6-1-4 حوكمة الأمن السيبراني

تستهدف هذه النقطة البحثية تحديد ماهية حوكمة الأمن السيبراني من حيث المفهوم، والأهداف، والضوابط، وذلك على النحو التالي:

6-1-4-1 مفهوم حوكمة الأمن السيبراني

لا يوجد تعريف محدد متفق عليه لمصطلح حوكمة الأمن السيبراني، فضلا عن ندرة الأبحاث العلمية التي تناولت هذا المصطلح، ولعل ذلك مرجعه هو حداثته النسبية. فقد عرفها المركز الوطني للأمن السيبراني (NCSC) بنيوزيلاندا بأنها " مجموعة من الأنشطة التي تمكن منشآت الأعمال من اتخاذ قرارات سليمة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية، بما يضمن الحفاظ على سرية وسلامة وتوافر المعلومات وكسب ثقة أصحاب المصالح" (NCSC 2021). وعرفها مركز أمن الإنترنت (CIS) بالولايات المتحدة الأمريكية بأنها " مجموعة من العمليات والإجراءات التي تساعد المؤسسات على اكتشاف الهجمات السيبرانية وتحديد كيفية الاستجابة لها ومنع حدوثها" (CIS 2021).

كما عرفتها دراسة (الزريقات، 2022) بأنها " المبادئ والقواعد والإجراءات المتبعة من جهة ما لضبط سلطات اتخاذ القرار، وتحديد أصحاب المسؤولية في تنفيذ المهام والواجبات ذات العلاقة بحماية الجهة من الهجمات الإلكترونية أو سوء استخدام الأصول المعلوماتية، مع ضمان استمرارية العمليات التشغيلية في حال وقوع حوادث سيبرانية." في حين عرفتها دراسة (Pullin, 2018) بأنها " ذلك الجزء من الحوكمة الذي يختص بمواجهة المخاطر السيبرانية في إطار إستراتيجية المنشأة وتوقعاتها المستقبلية."

وتخلص الباحثة من التعريفات السابقة لحوكمة الأمن السيبراني بأنها " مجموعة من الممارسات المناسبة لضبط وتوجيه أعمال المنشأة لتعزيز الأمن السيبراني والمرونة في مواجهة الهجمات الإلكترونية، بما يضمن منع أو التقليل من حدوثها، مع القدرة على إكتشافها والتعامل معها وسرعة التعافي من آثارها وتجنب تكرار حدوثها."

6-1-4-2 أهداف حوكمة الأمن السيبراني

تتعدد أهداف حوكمة الأمن السيبراني، ولعل من أهم هذه الأهداف ما يلي (الهيئة الوطنية للأمن السيبراني– المملكة العربية السعودية، 2018 ;NCSC, 2021 ;Qasaimeh and Jaradeh, 2022):

- التنسيق بين الإستراتيجية العامة للمنشأة وخطط العمل الخاصة بتطبيق إستراتيجية الأمن السيبراني، وبما يضمن تحقيق المتطلبات التنظيمية والتشريعية ذات العلاقة.
- ضمان توثيق ونشر متطلبات الأمن السيبراني والإلتزام المنشأة بها، مع التحديد الواضح للأدوار والمسئوليات لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني داخل المنشأة.
- تحديد وتوثيق وإعتماد منهجية شاملة لإدارة مخاطر الهجمات الإلكترونية التي تتعرض لها المنشأة، وذلك بما يضمن حماية الأصول المعلوماتية والتقنية الخاصة بها.
- ضمان تخصيص الموارد اللازمة للإستثمار في الأمن السيبراني، والتأكد من تضمين متطلبات الأمن السيبراني في منهجية إدارة مشاريع تطوير التطبيقات والبرمجيات الخاصة بالمنشأة.
- ضمان التأكد من أن العاملين بالمنشأة لديهم التوعية الأمنية اللازمة، وعلى دراية بمسئولياتهم في مجال الأمن السيبراني، وتزويدهم بالمهارات والمؤهلات والدورات التدريبية المطلوبة في هذا المجال لحماية الأصول المعلوماتية والتقنية للمنشأة .
- ضمان التأكد من المراجعة الدورية لتطبيق ضوابط الأمن السيبراني من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني داخل المنشأة، مع توثيق نتائج عملية المراجعة وعرضها على اللجنة الإشرافية للأمن السيبراني التابعة لمجلس الإدارة.
- التأكد من وجود نظام جيد لإعداد التقارير المتعلقة بالإفصاح عن الإمتثال لمتطلبات الأمن السيبراني وبرامج إدارة المخاطر السيبرانية وعلى رأسها مخاطر الهجمات الإلكترونية.

6-1-4-3 ضوابط حوكمة الأمن السيبراني

يتطلب تطبيق حوكمة الأمن السيبراني بمنشآت الأعمال الالتزام بمجموعة من الضوابط الرئيسية[1] هى؛ إستراتيجية الأمن السيبراني، وإدارة الأمن السيبراني، وسياسات وإجراءات الأمن السيبراني، وأدوار ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والأمن السيبراني ضمن إدارة المشاريع التقنية والمعلوماتية، والالتزام بتشريعات ومعايير الأمن السيبراني، والمراجعة والتدقيق الدوري للأمن السيبراني،

[1] يرجع في ذلك الى الملحق رقم (1)

والأمن السيبراني المتعلق بالموارد البشرية، والتدريب والتوعية بالأمن السيبراني (الضوابط الأساسية الصادرة عن الهيئة الوطنية للأمن السيبراني– المملكة العربية السعودية، 2018).

وفي هذا الصدد، تجدر الإشارة إلى أهمية إفصاح منشآت الأعمال عن إدارة مخاطر الأمن السيبراني، وذلك من خلال إعداد تقرير عن إدارة مخاطر الأمن السيبراني، لإيضاح الجهود المبذولة من قبل المنشأة في إدارة هذه المخاطر، باعتبار ذلك من الضوابط الهامة للحوكمة السيبرانية، والتي تقترح الباحثة إضافتها للضوابط السابق إيضاحها في الجدول رقم (1) السابق، خاصة وأن تطبيق ضوابط حوكمة الأمن السيبراني من شأنه تشجيع منشآت الأعمال على مثل هذا النوع من الإفصاح، إذ يمثل هذا التطبيق في حد ذاته، ذلك الجزء من الإفصاح الذي يعمل على بث إشارات إيجابية للسوق من خلال التواصل مع أصحاب المصالح بشأن الجهود المبذولة من قبل المنشأة لتقليل مخاطر الأمن السيبراني أو الحد منها ومنعها، وهو ما سوف تتناوله الباحثة في النقطة البحثية التالية.

6-1-5 الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني

يشير مصطلح مخاطر الأمن السيبراني إلى الخسائر المحتمل حدوثها؛ بسبب الهجمات الإلكترونية وما تحدثه من أضرار تتعلق بسرية ونزاهة وتوافر المعلومات، والتي تكبد منشآت الأعمال خسائر مالية كبيرة. وقد اهتم عدد من المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن مخاطر الأمن السيبراني وبرنامج إدارتها، ويأتي في مقدمتها الإرشادات الصادرة عن هيئة الأوراق المالية والبورصات الأمريكية The U.S. Securities and Exchange Commission (SEC) في2011م، والتي تم تحديثها في عام 2018م، كما قام المعهد الأمريكي للمحاسبين القانونيين The American Institute of Certified Public Accountants (AICPA) بوضع إطار للتقرير عن إدارة مخاطر الأمن السيبراني، وذلك لإرشاد منشآت الأعمال فيما يتعلق بتعزيز إفصاحتها المتعلقة بالأمن السيبراني. وجاء ذلك كاستجابة لشكاوى المستثمرين وغيرهم من أصحاب المصالح من عدم وجود معلومات كافية وفي الوقت المناسب عن مخاطر الأمن السيبراني التي تتعرض لها منشآت الأعمال، وجهودها في إدارة تلك المخاطر، وبالتالي عدم قدرتهم على تقييم موقف الأمن السيبراني لديها ومعرفة مدى فعالية برامجها في إدارة هذه النوعية من المخاطر (الرشيدى وعباس، 2019؛ SEC, 2011, 2018; Yang et al., 2020; AICPA, 2017). ويمكن إيضاح تلك الإرشادات على النحو التالي:

أ) إرشادات هيئة الأوراق المالية والبورصات الأمريكية (SEC)

اعتبرت هيئة الأوراق المالية والبورصات الأمريكية (SEC) أن الإفصاح عن مخاطر الأمن السيبراني وبرنامج إدارتها من أهم القضايا التي تتعلق بالحوكمة في مجال الأمن السيبراني (Sullivan & Cromwell LLP, 2022)، ولذلك أصدرت مجموعة من الإرشادات التوجيهية للشركات المدرجة بشأن متطلبات الإفصاح الاختياري عن تقرير إدارة مخاطر الأمن السيبراني في عام 2011م، وتم تحديثها في عام 2018م. وذلك لتعزيز وتوحيد الإفصاح في هذا المجال، ليشمل القواعد والعناصر الرئيسية للإفصاح عن إدارة مخاطر الأمن السيبراني[2] وهي؛ الأهمية النسبية، وعوامل الخطر، والموقف المالي ونتائج العمليات، ووصف طبيعة النشاط، والإجراءات القانونية، والإفصاح في القوائم المالية، ورؤية مجلس الإدارة (SEC, 2011, 2018).

وفي مارس 2022 أصدرت هيئة الأوراق المالية والبورصات الأمريكية (SEC) تعديلات على قواعدها بشأن متطلبات الإفصاح المتعلقة بإدارة مخاطر الأمن السيبراني، متضمنة الإفصاح بشكل دوري عن السياسات والإجراءات المتبعة لحوكمة مخاطر الأمن السيبراني، وتحديد المسؤول عن حوكمة الأمن السيبراني (SEC, 2022).

ب) إرشادات المعهد الأمريكي للمحاسبين القانونيين AICPA

في عام 2017م قدم المعهد الأمريكي للمحاسبين القانونيين (AICPA) إطار للتقرير عن إدارة مخاطر الأمن السيبراني لإرشاد منشآت الأعمال ودعمهم في إبلاغ المساهمين والعملاء وغيرهم من أصحاب المصالح، وفي الوقت المناسب عن الجهود المبذولة لإدارة مخاطر الأمن السيبراني، ومن ثم تعزيز الثقة المتبادلة بينهم. وأوصى الإطار المقدم بضرورة إفصاح منشآت الأعمال في تقرير إدارة مخاطر الأمن السيبراني عن ثلاث مجموعات من المعلومات، والتي يمكن إيضاحها على النحو التالي (AICPA, 2017):

المجموعة الأولى: معلومات عن برنامج إدارة مخاطر الأمن السيبراني

وتتضمن هذه المجموعة من المعلومات توصيف لطبيعة نشاط المنشأة، ووصف سردي لبرنامج إدارة مخاطر الأمن السيبراني بالمنشأة، والأهداف المتوقعة منه متضمنا معلومات عن هيكل حوكمة الأمن السيبراني، وطبيعة المخاطر السيبرانية التي تتعرض لها، ومعايير وسياسات الأمن السيبراني وما تشمله من ضوابط ومتطلبات.

[2] يرجع في ذلك الى الملحق رقم (2)

المجموعة الثانية: معلومات بشأن تأكيد الإدارة

وتتضمن هذه المجموعة من المعلومات تأكيدًا من إدارة المنشأة بشأن فعالية برنامج إدارة مخاطر الأمن السيبراني في تحقيق الأهداف السيبرانية التي يسعى إلى تحقيقها، وأن إعداد تقرير إدارة مخاطر الأمن السيبراني قد تم وفقا لمتطلبات الإطار الذي وضعه المعهد الأمريكي للمحاسبين القانونيين.

المجموعة الثالثة: رأي مراقب الحسابات

حيث يتطلب الأمر ضرورة إبداء مراقب الحسابات رأيه بشأن تقرير إدارة مخاطر الأمن السيبراني ومدى فعالية تطبيق ضوابط الأمن السيبراني بالمنشأة.

وفي هذا الصدد، قامت أيضا إدارة الأوراق المالية الكندية The Canadian Securities Administrators (CSA) – وهي هيئة رقابية كندية تابعة لسوق المال – بإصدار إرشادات في عام 2017م للشركات المقيدة بالبورصة للإفصاح عن مخاطر الأمن السيبراني وبرنامج إدارتها، وذلك من حيث مصدر وطبيعة تلك المخاطر، والآثار المحتملة للهجمات الإلكترونية، وخطط التعافي من آثار تلك الهجمات سواء السابقة أو المستقبلية، وأيضا الحوكمة ودورها في الحد من هذه المخاطر (CSA, 2017).

الأمر الذي يؤكد اهتمام المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن إدارة مخاطر الأمن السيبراني، كآلية هامة للحوكمة السيبرانية تعمل على حث، وتشجيع الشركات والمؤسسات المالية الأكثر استهدافًا من قبل الهجمات الإلكترونية، على هيكلة الضوابط الأساسية للأمن السيبراني، والتي يأتي على رأسها تبنى إستراتيجية متكاملة للحوكمة السيبرانية تمكنها من تحديد مخاطر الهجمات الإلكترونية وإدارتها ومراجعتها، وذلك حتى يمكنها توفير الإفصاح المناسب للمساهمين وغيرهم من أصحاب المصالح عن جهود المنشأة في هذا المجال، ومن ثم تعزيز ودعم ثقتهم بها. الأمر الذي يعمل على زيادة قدرتها التنافسية، ومن ثم تحسين أدائها المالي– وبصفة خاصة في القطاع المصرفي– وذلك كما يتضح من النقطة البحثية التالية.

6-1-6 الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل تطبيق حوكمة الأمن السيبراني ودوره في تحسين الأداء المالي

يمكن تعريف الأداء المالي بأنه ذلك الأداء الذي يسهم في توفير الموارد المالية، ويعمل على تزويد المنشأة بالفرص الاستثمارية، وتلبية رغبات العملاء وغيرهم من أصحاب المصالح، وأيضا تحديد مدى قدرة المنشأة على تحقيق الأهداف المالية المخططة وخلق القيمة ومجابهة المستقبل (Ayuba et al., 2019; Tudose et al., 2022; Meiryani et al., 2023). ونظرا لأن الهجمات الإلكترونية وغيرها من

الحوادث السيبرانية تؤدي إلى تخريب، أو تعطيل، أو التلاعب بنظم المعلومات بمنشآت الأعمال، مما يؤثر سلبا على ملائمة وموثوقية معلوماتها المالية وغير المالية، وبالتالي جودتها وتحملها خسائر مالية كبيرة (حامد وآخرون، 2021؛ Skinner, 2019; Akinbowale, 2020; Yang et al., 2020; Bukht et al., 2020; Maleh et al., 2021; Qasaimeh and Jaradeh, 2022; Ali et al., 2022; Bongiovanni et al., 2022)، فمن المتوقع – من وجهة نظر الباحثة– أن الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن السيبراني، من شأنه الحفاظ على ملائمة وموثوقية المعلومات المالية، وبالتالي زيادة جودتها، ومن ثم تحسين الأداء المالي، وبصفة خاصة البنوك باعتبار أنها من أكثر منشآت الأعمال استهدافًا بالهجمات الإلكترونية.

إذ يمكن أن تلعب حوكمة الأمن السيبراني دورا هاما في تعزيز قدرة البنوك – وغيرها من منشآت الأعمال – على دعم أمنها السيبراني ومواجهة الهجمات الإلكترونية، ومن ثم تعزيز قدرتها التنافسية بما يسهم في تحسين أدائها المالي، وذلك نظرا لدورها البارز في تحقيق ما يلى (Bukht et al., 2020; Maleh et al., 2021; Qasaimeh and Jaradeh, 2022; Bongiovanni et al. 2022):

- تطوير إستراتيجية الأمن السيبراني بالبنك للحفاظ على سرية المعلومات وصحتها وتوافرها، وبالتالي الحفاظ على سمعة البنك وزيادة ثقة المتعاملين معه.
- العمل على تحقيق التوافق والاتساق بين أهداف البنك ومتطلبات تحقيق الأمن السيبراني وهو ما يؤدي إلى زيادة جودة الخدمات المصرفية المقدمة، ومن ثم زيادة ملائمة وموثوقية المعلومات المالية، مما يؤدي إلى جذب مزيد من العملاء وتحقيق قدر أكبر من العوائد.
- إدارة مشروعات تكنولوجيا المعلومات بالبنك مع مراعاة متطلبات تحسين الأنشطة والخدمات المقدمة وبالتالي زيادة رضاء العملاء الحاليين وجذب مزيد من العملاء المستقبليين.
- العمل على الحد من الغش والتلاعب المالي الإلكتروني، ومن ثم زيادة القدرة على إنتاج قوائم وتقارير مالية تتسم بالشفافية والمصداقية، مما ينعكس بالإيجاب على كفاءة الأداء المالي للبنك.
- العمل على رفع كفاءة نظم الرقابة والمراجعة الداخلية وتحسين قدرتها على متابعة وتقييم ضوابط الأمن السيبراني لحماية أمن المعلومات المالية، مما يسهم في تحسين الأداء المالي للبنك.
- توفير التوعية والتدريب اللازم في مجال الأمن السيبراني لجميع الأطراف ذات الصلة بالبنك، مما يعمل على تخفيض التكاليف والوقت والجهد الذي تحتاج إليه عمليات تحليل وتخزين وتشغيل البيانات المالية واستراجاعها بشكل آمن وبالتالي زيادة كفاءة الأداء المالي للبنك.

- تعزيز المساءلة من خلال التحديد الواضح للأدوار والمسؤوليات الخاصة بالأمن السيبراني؛ مما يسهم في رفع كفاءة أنظمة تكنولوجيا المعلومات بالبنك، وبالتالي كفاءة المنتجات والخدمات المقدمة للعملاء.
- المراجعة الدورية لضوابط الأمن السيبراني بالبنك لتوفير الحماية اللازمة للمتعاملين معه من مخاطر الهجمات الإلكترونية، وهو ما يزيد درجة الثقة لدى العملاء فى جودة المعاملات المالية الرقمية مع البنك وقدرته على تحقيق أهدافه.
- العمل على الاشتراك في برامج لتعزيز التثقيف والوعي المالي السيبراني للعملاء وجميع أفراد المجتمع للوقاية من مخاطر الهجمات الإلكترونية، مما يسهم في تحسين صورة البنك أمام المجتمع بصفة عامة والعملاء والمستثمرين بصفة خاصة ويعمل على توسيع قاعدة العملاء لدى البنك.

وفي هذا الصدد، ترى الباحثة أن مثل هذا الدور البارز الذي يمكن أن تلعبه حوكمة الأمن السيبراني في دعم الأمن السيبراني لمنشأة الأعمال، هو نفسه ما يمكن أن يكون بمثابة تشجيع لتلك المنشآت على تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني لإبراز جهودها في هذا المجال، واعتبار ذلك من الضوابط الهامة لحوكمة الأمن السيبراني، خاصة وقد اتفقت كثير من الدراسات على أهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني (Li et al., 2018; Frank et al., 2018; Cheong et al., 2021; Kelton, 2021)، إذ أوضحت تلك الدراسات أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني من شأنه زيادة المصداقية والثقة بأداء منشآت الأعمال، وزيادة قدرة المساهمين وغيرهم من أصحاب المصالح على تقييم أداء منشآت الأعمال وجهودها في مواجهة مخاطر الأمن السيبراني، وبالتالي تقليل حالة عدم التأكد وجذب مزيد من المستثمرين، إلى جانب تقليل تكاليف التقاضي التي قد تتعرض لها المنشأة.

كما اتفقت كثير من الدراسات على أهمية إدارة مخاطر الأمن السيبراني والإفصاح عنها في تحسين الأداء المالي للبنوك، حيث أوضحت تلك الدراسات أن هذا النوع من الإفصاح في التقارير المالية للبنوك، يعتبر بمثابة تأكيد على امتثالها للمتطلبات القانونية والتنظيمية المتعلقة بالأمن السيبراني. كما يعمل على إبراز جهود البنك وقدرته على مواجهة الهجمات الإلكترونية، بما يساعد على زيادة شفافية ووضوح التعامل مع البنك، وبالتالي تمكين العملاء وغيرهم من أصحاب المصالح من تقييم قدرة تلك البنوك على التصدي للتهديدات السيبرانية ومعالجتها، ومن ثم تعزيز الثقة بالخدمات المصرفية المقدمة، وهو ما يعمل بدوره على جذب مزيد من العملاء، وبالتالي زيادة المدخرات وارتفاع نسب السيولة لدى البنك ومن ثم تحسين أدائه المالي(قاسم ورشوان، 2022؛ أحمد، 2023؛ أبو سمك، 2023؛ Gatzert and Schubert, 2022; Mazumder and Hossain, 2022).

وفي سياق متصل، يرى البعض أن الإفصاح عن إجراءات الأمن السيبراني يعمل على تحسين العمليات الداخلية وتعزيز الوعي بأمن المعلومات لدى المستخدمين، خاصة وأن انخفاض الوعي التكنولوجي للمستخدم يعد إحدى المعوقات الرئيسية في سبيل تحقيق الإدارة الفعالة لمخاطر الأمن السيبراني، مما يسهم في تحسين صورة البنك أمام المجتمع بصفة عامة والعملاء والمستثمرين بصفة خاصة. كما أنه يسهم في تعزيز الحوكمة المؤسسية وإدارة المخاطر بشكل فعال؛ ومن ثم المساهمة في تحقيق الاستقرار المالي للقطاع المصرفي (الأمير، 2022؛ Panda and Bower, 2020).

إلا أنه على النقيض مما سبق، يرى بعض الباحثين (Ettredge et al., 2018; Li et al., 2018; Walton et al., 2021; Cheng et al., 2022) أن الإفصاح عن إدارة مخاطر الأمن السيبراني يعد سلاحًا ذا حدين، حيث وإن كان يحقق العديد من المنافع – كما سبق وأوضحت الباحثة – إلا أنه يثير المخاوف بشأن احتمال وقوع حوادث سيبرانية في المستقبل، وذلك حال استغلال المهاجمين للمعلومات المتعلقة بحوادث الأمن السيبراني المفصح عنها، والإجراءات المضادة التي تتخذها المنشأة لمواجهتها، والبحث عن ثغرات جديدة لمهاجمة تلك المنشآت وتهديد أمنها السيبراني. فضلا عن المخاوف بشأن استغلال المديرين للسطلة الممنوحة لهم في إخفاء المعلومات والأخبار المتعلقة بحوادث الأمن السيبراني لتجنب المخاطر المحتملة المتعلقة بالإفصاح عن مخاطر الأمن السيبراني، مما يزيد بدوره من مشكلة عدم تماثل المعلومات. كما يرى بعض الباحثين (Goel and Shawky, 2014; Berkman et al., 2018; Tosun, 2021) أن الإفصاح عن مخاطر الأمن السيبراني قد يحمل في طياته نغمة سلبية تنعكس على تقييم المستثمرين لأداء الشركة، وأن الإعلان عن حدوث هجمات سيبرانية يزيد خطر انخفاض العوائد اليومية، ويؤثر سلبا على أحجام التداول.

وتأسيسا على ما تقدم، تؤيد الباحثة الاتجاه المنادي بضرورة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، حيث من شأنه تحقيق العديد من المنافع، والتي تؤدي إلى تحسين الأداء المالي لمنشآت الأعمال وبصفة خاصة البنوك، على أن يتم ذلك الإفصاح في ظل تطبيق إطار فعال للحوكمة السيبرانية يعمل على دعم وتعزيز الأمن السيبراني للمنشأة بشكل مستمر، ومن ثم التغلب على المخاوف المصاحبة لهذا النوع من الإفصاح. وتمهيدا لاشتقاق فروض تلك العلاقات واختبارها، سوف تقدم الباحثة عرض موجز لأهم الدراسات السابقة التي تناولت تلك المتغيرات، وذلك من خلال الجزئية التالية من هذا البحث.

6-2 الدراسات السابقة وإشتقاق فروض البحث

6-2-1 مقدمة

ظهرت في الآونة الأخيرة بعض الدراسات التي اهتمت ببحث سبل وآليات تعزيز الأمن السيبراني ومواجهة الهجمات الإلكترونية بمنشآت الأعمال وبصفة خاصة بالبنوك وذلك لضمان التحول الرقمي الآمن، فضلا عن تناول أهمية حوكمة الأمن السيبراني والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني. وللوقوف على الترابط فيما بين هذه الدراسات لاستكمال جهود الباحثين في هذا المجال، إلى جانب عرض وتحليل العلاقات بين متغيرات الدراسة بغرض اشتقاق وتطوير فروض البحث، سوف تقوم الباحثة من خلال هذه الجزئية باستعراض موجز لهذه الدراسات، وذلك على النحو التالي:

6-2-2 الدراسات التي تناولت العلاقة بين حوكمة الأمن السيبراني والأمن السيبراني

أيدت الدراسات السابقة التي تناولت العلاقة بين حوكمة الأمن السيبراني والأمن السيبراني، الدور الإيجابي الذي يمكن أن تلعبه حوكمة الأمن السيبراني في تعزيز الأمن السيبراني لمنشآت الأعمال، ومنها دراسة (Solms and Solms, 2018) والتي استهدفت إلقاء الضوء على مفهومي الأمن السيبراني وحوكمة الأمن السيبراني مع تحديد واجبات ومسؤوليات مجالس إدارات الشركات وإداراتها التنفيذية في هذا المجال، وذلك في ضوء المعيارين؛ (ISO/IEC 27032) المتعلق بالأمن السيبراني لمنشآت الأعمال، و(ISO/IEC 27014) المتعلق بحوكمة أمن المعلومات. وقد اتبعت الدراسة منهجية البحث الثانوي، وتوصلت لعدد من النتائج لعل من أهمها؛ أولا: تعتبر حوكمة الأمن السيبراني جزءًا من حوكمة أمن المعلومات، حيث يهتم أمن المعلومات بحماية البيانات والمعلومات، سواء كانت رقمية أو غير رقمية من أي استخدام غير مصرح به، في حين يهتم الأمن السيبراني بحماية كل ما هو متعلق بالإنترنت سواء بيانات أو شبكات أو أجهزة من أي هجمات إلكترونية. ثانيا: يقع على عاتق أعضاء مجالس إدارات الشركات وإدارتها التنفيذية فهم ماهية الأمن السيبراني، وعلاقته بأمن المعلومات مع ضرورة وضع إستراتيجية واضحة لحوكمة الأمن السيبراني لتوفير الحماية من المخاطر السيبرانية.

كما استهدفت دراسة (De Matos, 2019) استكشاف أثر حوكمة الأمن السيبراني على العلاقات بين منشآت الأعمال وأصحاب المصالح، وذلك من خلال إجراء دراسة ميدانية استهدفت عينة مكونة من 116 متخصص في الأمن السيبراني بقطاعات مختلفة، وفي دول مختلفة. وقد توصلت الدراسة إلى عدد من النتائج لعل من أهمها؛ أولا: أن الهجمات السيبرانية قد أصبحت من أخطر التهديدات التي تواجه منشآت الأعمال، والتي تؤثر فى عملياتها اليومية وعلاقاتها مع أصحاب المصالح. ثانيا: تلعب حوكمة الأمن

السيبراني دورا بارزا في التصدي للهجمات السيبرانية وتحسين صورة المنشأة والحفاظ على سمعتها أمام أصحاب المصالح. وهو ما أيدته دراسة (Al Tahat and Abdel Moneim, 2020) والتي استهدفت استكشاف أثر تطبيقات الذكاء الاصطناعى على تطبيق حوكمة الأمن السيبراني في البنوك التجارية الأردنية، وذلك من خلال إجراء دراسة ميدانية استهدفت العاملين بمكاتب المراجعة الخارجية ممن لديهم خبرة بمجال المراجعة للبنوك التجارية الأردنية، والتي بلغ عددها في هذه الدراسة 13 بنكًا. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ أولا: أصدر البنك المركزي الأردني تعليماته للبنوك التجارية الأردنية بتطبيق حوكمة الأمن السيبراني لمواجهة مخاطر تكنولوجيا المعلومات. ثانيا: وجود تأثير إيجابي لتطبيقات الذكاء الإصطناعي على التطبيق الصحيح للحوكمة السيبرانية في البنوك التجارية الأردنية.

وفي سياق متصل، استهدفت دراسة (Albalas et al., 2022) إلقاء الضوء على أهمية الأمن السيبراني وحوكمة الأمن السيبراني في ظل التحول الرقمي لمنشآت الأعمال. وقد اتبعت الدراسة منهجية البحث الثانوي، وتوصلت لعدد من النتائج لعل من أهمها؛ أولا: يعتبر مفهوم حوكمة الأمن السيبراني من المفاهيم الحديثة في مجال الأمن السيبراني، والتي حظيت باهتمام كثير من دول العالم، ودخلت حيز التطبيق في عدد كبير منها في محاولة للتصدي للحوادث السيبرانية التي تتعرض لها منشآت الأعمال وبصفة خاصة قطاع الخدمات المالية. ثانيا: يجب على منشآت الأعمال اتباع نهج استباقي لتعزيز أمنها السيبراني، على أن يتضمن ذلك إجراء تقييم سنوي للمخاطر، وذلك لفهم بيئتها السيبرانية واكتساب فهم شامل لمخاطرها. وأيضا استهدفت دراسة (Qasaimeh and Jaradeh, 2022) تحليل أثر الذكاء الاصطناعي على فعالية تطبيق حوكمة الأمن السيبراني بالبنوك التجارية الأردنية. وذلك من خلال إجراء دراسة ميدانية استهدفت عينة مكونة من 208 مفردة من الموظفين بأقسام المحاسبة، والمراجعين الداخليين، والمبرمجين بالبنوك التجارية الأردنية المدرجة بسوق عمان لتداول الأوراق المالية. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ أولا: تسهم حوكمة الأمن السيبراني في تحسين جودة الخدمات المصرفية الإلكترونية المقدمة للعملاء. ثانيا: تسهم تطبيقات الذكاء الاصطناعي (النظم الخبيرة والشبكات العصبية والخوارزميات الجينية) في تعزيز فعالية تطبيق حوكمة الأمن السيبراني بالبنوك التجارية الأردنية.

كما استهدفت دراسة (جمال وبن عيسى، 2022) إبراز أهمية حوكمة الأمن السيبراني مع استعراض الجهود المبذولة من قبل دولة الجزائر فيما يتعلق بحوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية. وقد اتبعت الدراسة منهجية البحث الثانوي، وتوصلت لعدد من النتائج لعل من أهمها؛ أولا: تعتبر قضية الأمن السيبراني من التحديات الصعبة التي تواجهها دولة الجزائر في ظل تنامي التهديدات والهجمات الإلكترونية المصاحبة للتوسع في التحول الرقمي للخدمات العمومية، مما يتطلب

تطبيق حوكمة الأمن السيبراني لضمان الثقة في هذه الخدمات. ثانيا: غياب مفهوم حوكمة الأمن السيبراني بين مختلف مصالح وهيئات القطاع العمومي الجزائري مما يتطلب ضرورة الاستفادة من تجارب الدول الرائدة في مجال الأمن السيبراني والاستعانة بالنماذج والمعايير العالمية للاستفادة منها في وضع برنامج لحوكمة الأمن السيبراني. وهو ما يتفق مع دراسة (Mijwil et al., 2023) والتي استهدفت أيضا إبراز أهمية حوكمة الأمن السيبراني في مواجهة التهديدات الإلكترونية في ظل التحول الرقمي للخدمات العامة بالعديد من الدول. وقد اتبعت الدراسة منهجية البحث الثانوى، وتوصلت لعدد من النتائج لعل من أهمها؛ أولا: يعتبر الأمن السيبراني من أبرز التحديات التي تواجه حكومات الدول في مسيرة التحول الرقمي، وذلك نظرا لزيادة حدة الهجمات الإلكترونية على مختلف القطاعات، والتي تكمن خطورتها في اعتمادها على تقنيات حديثة ومتطورة، فضلا عن سهولة وسرعة انتشارها، إلى جانب اتساع نطاق تأثيرها في وقت قصير وعن بعد. ثانيا: تعتبر حوكمة الأمن السيبراني جزء بالغ الأهمية في الإدارة الشاملة للمخاطر بمنشآت الأعمال لحماية أنظمة المعلومات من التهديدات السيبرانية.

وفي سياق متصل، استهدفت دراسة (محمد ، 2023) قياس المقدرة التقييمية المباشرة وغير المباشرة للإفصاح عن ضوابط حوكمة الأمن السيبراني وتأثيره على قرارات المستثمرين، وذلك من خلال إجراء دراسة تطبيقية استهدفت تحليل محتوى التقارير المالية لشركتى زين و STC بالمملكة العربية السعودية، خلال الفترة من عام 2019 إلى 2022. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ أولا: يتطلب تطبيق ضوابط حوكمة الأمن السيبراني تفعيل مجموعة من الممارسات على مستوى الأفراد والعمليات والأنظمة الأمنية بالمنشأة لتعزيز أمنها السيبراني. ثانيا: وجود مقدرة تقييمية مباشرة للإفصاح عن ضوابط حوكمة الأمن السيبراني. ثالثا: وجود تأثير معنوي للإفصاح عن ضوابط حوكمة الأمن السيبراني على قرارات المستثمرين.

وتأسيسًا على ما تقدم، يتضح للباحثة؛ أولاً: قلة عدد الدراسات التي اهتمت بدراسة العلاقة بين حوكمة الأمن السيبراني والأمن السيبراني، مع عدم اهتمام أي من الدراسات السابقة بتناول تلك العلاقة في البيئة المصرية وبصفة خاصة في قطاع البنوك (في حدود ما اطلعت عليه الباحثة)، الأمر الذي يتطلب مزيدًا من الدراسة والتحليل لتلك العلاقة في البيئة المصرية. ثانيا: إتفاق نتائج الدراسات السابقة على وجود تأثير إيجابي للحوكمة السيبرانية على الأمن السيبراني لمنشآت الأعمال. وتؤيد الباحثة هذه النتائج وبصفة خاصة في قطاع البنوك باعتبار أنه من أكثر القطاعات المستهدفة بالهجمات الإلكترونية، وبالتالي أصبح ضرورة العمل على تعزيز قدرات البنوك في مواجهة الهجمات الإلكترونية أمرًا حتميًا، خاصة في ظل

التحول نحو الصيرفة الرقمية والتوسع في تقديم الخدمات والمنتجات الإلكترونية، ولذلك يمكن للباحثة إشتقاق الفرض التالي:

H_1: تساهم حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية.

6-2-3 الدراسات التي تناولت جدوى الإفصاح عن إدارة مخاطر الأمن السيبراني وعلاقته بالأداء المالي

تباينت الآراء فيما يتعلق بطبيعة العلاقة بين الإفصاح عن إدارة مخاطر الأمن السيبراني والأداء المالي لمنشآت الأعمال، إذ يرى البعض أن الإفصاح عن إدارة مخاطر الأمن السيبراني من شأنه زيادة المصداقية والثقة بأداء منشآت الأعمال، وزيادة قدرة المساهمين وغيرهم من أصحاب المصالح على تقييم أداء تلك المنشآت وجهودها في مواجهة مخاطر الأمن السيبراني، ومن ثم تقليل حالة عدم التأكد وجذب مزيد من المستثمرين، إلى جانب تقليل تكاليف التقاضي التي قد تتعرض لها المنشأة، وهو ما يمكن أن يؤدي بدوره إلى تحسين أدائها المالي. ومن الدراسات المؤيدة لهذا الاتجاه؛ دراسة (قاسم ورشوان، 2022) والتي استهدفت استكشاف إثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي للبنوك، وذلك من خلال إجراء دراسة ميدانية استهدفت عينة مكونة من 120 مفردة من المدراء الماليين ومدراء الفروع ومدراء إدارات المخاطر بالبنوك المدرجة ببورصة فلسطين. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ وجود أثر معنوي لإدارة مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي للبنوك المدرجة ببورصة فلسطين، وأوصت الدراسة بضرورة قيام البنوك بوضع نماذج فعالة لإدارة المخاطر السيبرانية المصاحبة لتكنولوجيا المعلومات، وهو ما يتطلب الرقابة المستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

وفي سياق متصل، استهدفت دراسة (Gatzert and Schubert, 2022) اختبار محددات إدارة مخاطر الأمن السيبراني وأثرها على قيمة المنشأة. وذلك من خلال إجراء دراسة تطبيقية استهدفت تحليل محتوى التقارير المالية لعينة من البنوك وشركات التأمين الأمريكية خلال الفترة من 2011 إلى 2018. وقد توصلت الدراسة إلى عدد من النتائج منها؛ وجود ارتباط إيجابي معنوي بين إدارة مخاطر الأمن السيبراني وقيمة المنشأة بالاعتماد على نموذج Tobin's Q. كما استهدفت دراسة (Masoud and Al-Utaibi, 2022) اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على تحسين جودة التقارير المالية. وذلك من خلال إجراء دراسة تطبيقية على عينة من الشركات الأمريكية خلال الفترة من 2006 إلى 2016. وقد توصلت الدراسة لعدد من النتائج منها؛ وجود ارتباط إيجابي بين الإفصاح عن تقرير

إدارة مخاطر الأمن السيبراني وتحسين جودة التقارير المالية وهو ما ينعكس ايجابيًا على جودة عملية المراجعة.

كما استهدفت دراسة (Mazumder and Hossain, 2022) قياس مدى إفصاح البنوك في بنغلاديش عن تقرير إدارة مخاطر الأمن السيبراني، إلى جانب فحص العلاقة بين خصائص تكوين مجلس الإدارة (الحجم، الاستقلالية، التنوع بين الجنسين) والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني. وذلك من خلال إجراء دراسة تطبيقية استهدفت تحليل محتوى التقارير المالية لعينة من البنوك التجارية المدرجة في بورصة بنغلاديش خلال الفترة من 2014 إلى 2020. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ أولا: وجود اتجاه متزايد للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني من قبل البنوك التجارية المدرجة في بورصة بنغلاديش خلال الفترة من 2014 إلى 2020. ثانيا: وجود علاقة ارتباط موجبة بين خصائص تكوين مجلس الإدارة من حيث الحجم وزيادة عدد الإناث بالمجلس والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني. ثالثا: وجود علاقة ارتباط موجبة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وربحية البنك والتي تم قياسها بنسبة صافي الربح بعد الضرائب إلى إجمالي الأصول، حيث أوضحت الدراسة أن البنوك ذات الربحية الأعلى تميل إلى استرضاء أصحاب المصلحة واكتساب ثقتهم من خلال تقديم المزيد من المعلومات حول الأمن السيبراني.

وفي ذات السياق، استهدفت دراسة (أحمد، 2023) قياس أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي للبنوك. وذلك من خلال إجراء دراسة تطبيقية على البنوك التجارية السعودية خلال الفترة من 2018 إلى 2022. وقد توصلت الدراسة لعدد من النتائج لعل من أهمها؛ وجود تأثير طردي معنوي للعلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إدارة مخاطر الأمن السيبراني على الأداء المالي للبنك. كما استهدفت دراسة (على وعلى، 2022) اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. وذلك من خلال إجراء دراسة تجريبية على عينة من المستثمرين بالأسهم والمحللين الماليين بشركات السمسرة. وقد خلصت الدراسة إلى وجود تأثير إيجابي معنوي لتقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار في الأسهم، كونه يضفي الثقة على أعمال الشركة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية. مما يمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل، مما يسهم في ترشيد قرارات المستثمرين وتحسين جودة أحكامهم الاستثمارية. وهو ما أيدته دراسة (شرف، 2023) والتي استهدفت أيضا اختبار أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات

المستثمرين المصريين غير المحترفين. وذلك من خلال إجراء دراسة تجريبية على عينة من أعضاء هيئة التدريس وطلبة الدراسات العليا بكليات التجارة بالجامعات المصرية، كممثلين للمستثمرين غير المحترفين. وقد خلصت الدراسة إلى وجود تأثير إيجابي معنوي لإفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين.

وفي سياق متصل، استهدفت دراسة (أبو سمك، 2023) اختبار أثر الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح. وذلك من خلال إجراء دراسة تطبيقية على البنوك المدرجة بالبورصة المصرية خلال الفترة من 2018 إلى 2022. وقد توصلت الدراسة لعدد من النتائج هي؛ أولا: وجود تأثير طردي ذي دلالة إحصائية لمستويات الإفصاح عن مخاطر الأمن السيبراني باستخدام القابلية للقراءة على استجابة أسعار الأسهم عقب إعلانات الأرباح. ثانيا: وجود تأثير طردي ذي دلالة إحصائية لمستويات الإفصاح عن مخاطر الأمن السيبراني باستخدام لغة التقاضي على استجابة أسعار الأسهم عقب إعلانات الأرباح. وقد أوصت الدراسة بضرورة توفير إطار عمل للإفصاح عن مخاطر الأمن السيبراني لكي يستطيع المستثمرون معرفة وضع المؤسسة تجاه مخاطر الأمن السيبراني. كما استهدفت دراسة (Elnagar et al., 2024) اختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على جودة التقارير المالية والقيمة السوقية لمنشآت الأعمال. وذلك من خلال إجراء دراسة تطبيقية على عينة من شركات قطاع الاتصالات وتكنولوجيا المعلومات المقيدة بالبورصة المصرية خلال الفترة من 2017 إلى 2022. وقد خلصت نتائج الدراسة إلى وجود تأثير إيجابي معنوي للإفصاح عن إدارة مخاطر الأمن السيبراني على جودة التقارير المالية والقيمة السوقية لمنشآت الأعمال.

إلا أنه على الجانب الآخر، أوضحت بعض الدراسات أن الإفصاح عن مخاطر الأمن السيبراني قد يزيد من احتمالات تعرض المنشأة لاختراقات مستقبلية، كما أنه قد يحمل في طياته نغمة سلبية تنعكس على تقييم المستثمرين لأداء المنشآت، وأن الإعلان عن حدوث هجمات سيبرانية يزيد من خطر انخفاض العوائد اليومية ويؤثر سلبا على أحجام التداول. ومن هذه الدراسات؛ دراسة (Ettredge et al., 2018) والتي استهدفت اختبار العلاقة بين الإفصاح عن المخاطر السيبرانية وتعرض المنشأة للاختراقات السيبرانية في المستقبل. وذلك من خلال إجراء دراسة تطبيقية استهدفت تحليل محتوى التقارير المالية لعينتين من الشركات الأمريكية، إحداهما تعرضت لهجمات سيبرانية وأفصحت عنها، والأخرى تعرضت لهجمات سيبرانية ولم تفصح عنها، وذلك خلال الفترة من 2007 إلى 2015. وقد خلصت نتائج الدراسة إلى وجود ارتباط إيجابي معنوي بين الإفصاح عن مخاطر الأمن السيبراني والتعرض لاختراقات سيبرانية في المستقبل. كما استهدفت دراسة (Berkman et al., 2018) قياس أثر الوعي بالأمن السيبراني على

القيمة السوقية لمنشآت الأعمال. وذلك من خلال إجراء دراسة تطبيقية استهدفت تحليل محتوى التقارير المالية لعينة من الشركات الأمريكية المدرجة في مؤشر the Russell 3000 خلال الفترة من 2012 إلى 2016. وقد توصلت الدراسة لعدد من النتائج منها؛ أن نغمة الإفصاح عن مخاطر الأمن السيبراني باستخدام كلمات سلبية، يمكن أن تؤثر بشكل سلبي على القيمة السوقية لمنشآت الأعمال.

وفي سياق متصل، استهدفت دراسة (Li et al., 2018) اختبار أثر الإفصاح عن مخاطر الأمن السيبراني على احتمال حدوث حوادث سيبرانية في المستقبل. وذلك من خلال إجراء دراسة تطبيقية عينة من الشركات الأمريكية المدرجة بالبورصة خلال الفترة من 2005 إلى 2015. وقد توصلت الدراسة لعدد من النتائج منها؛ وجود ارتباط إيجابي معنوي بين الإفصاح عن مخاطر الأمن السيبراني واحتمال حدوث حوادث سيبرانية في المستقبل. كما استهدفت دراسة (Tosun, 2021) اختبار أثر الإفصاح عن الهجمات السيبرانية على العوائد اليومية للأسهم وأحجام التداول. وذلك من خلال إجراء دراسة تطبيقية على عينة من الشركات الأمريكية المدرجة بالبورصة خلال الفترة من 2004 إلى 2019. وقد خلصت نتائج الدراسة إلى وجود تأثير سلبي للإفصاح عن الهجمات السيبرانية على العوائد اليومية للأسهم وأحجام التداول، حيث أوضحت الدراسة أن الإفصاح عن الاختراقات السيبرانية يعتبر بمثابة صدمة سلبية غير متوقعة لسمعة المنشأة، تدفع المستثمرين لسرعة التخلص من أسهمها بالبيع. وهو ما يتفق مع ما توصلت إليه دراسة (Cheng et al., 2022) والتي استهدفت اختبار أثر الإفصاح عن مخاطر الأمن السيبراني على قرارات المستثمرين غير المحترفين. وذلك من خلال إجراء دراسة تجريبية استهدفت عينة من الطلاب بالولايات المتحدة الأمريكية ممن لديهم خبرة استثمارية لا تقل عن ثلاث سنوات، وحصلوا على دورتين تدريبيتين على الأقل في المحاسبة والتمويل، وبلغ حجم العينة 112 طالبا وطالبة، تم تجميعهم عن طريق منصة Amazon Mechanical Turk (M-Turk) ، كممثلين للمستثمرين غير المحترفين. وقد خلصت نتائج الدراسة إلى وجود تأثير سلبي للإفصاح عن مخاطر الأمن السيبراني على قرارات المستثمرين غير المحترفين، حيث أوضحت الدراسة أن المستثمرين غير المحترفين أقل ميلا للاستثمار في الشركات التي تعرضت لاختراقات سيبرانية.

وفي ذات السياق، استهدفت دراسة (يوسف، 2022) التعرف على واقع الإفصاح عن إدارة مخاطر الأمن السيبراني، وأثره على قرارات الاستثمار ومنح الائتمان. وذلك من خلال إجراء دراسة ميدانية استهدفت مدراء ونواب مدراء إدارة المخاطر في عدد من الشركات المدرجة بالبورصة المصرية. وقد توصلت الدراسة لعدد من النتائج منها؛ أولا: عدم إفصاح الشركات المدرجة بالبورصة المصرية عن تقرير

إدارة مخاطر الأمن السيبراني مع عدم وجود نموذج محدد للإفصاح. ثانيا: يرى المشاركون في الاستقصاء أن الإفصاح عن مخاطر الأمن السيبراني قد يضر بمصالح الشركة واستثماراتها.

وتأسيسًا على ما تقدم، يتضح للباحثة؛ أولاً: تباين نتائج الدراسات السابقة التي تناولت جدوى الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وعلاقته بالأداء المالي، حيث ولا تزال العلاقة بينهما محل دراسة وجدل ونقاش لم يحسم بعد. ثانيًا: ندرة الدراسات التي اهتمت بدراسة العلاقة بين الإفصاح عن إدارة مخاطر الأمن السيبراني وعلاقته بالأداء المالي في البنوك بالبيئة المصرية (في حدود ما اطلعت عليه الباحثة)، الأمر الذي يتطلب مزيدًا من الدراسة والتحليل لتلك العلاقة في مصر. ثالثا: عدم اهتمام الدراسات السابقة (في حدود ما اطلعت عليه الباحثة) بتناول أثر تطبيق ضوابط حوكمة الأمن السيبراني على الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية، الأمر الذي يتطلب دراسة وتحليل تلك العلاقة. رابعا: تتوقع الباحثة وجود تأثير إيجابي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على الأداء المالي للبنوك، وخاصة في ظل تطبيق ضوابط حوكمة الأمن السيبراني، نظرا لدورها في تعزيز ودعم الأمن السيبراني ومواجهة الهجمات الإلكترونية في منشآت الأعمال، ومن ثم تعزيز قدرتها التنافسية بما يسهم في تحسين أدائها المالي. ولذلك يمكن للباحثة اشتقاق الفروض التالية:

H_2: تساهم حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية.

H_3: يساهم الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

6- 3 الدراسة التجريبية

6-3-1 مقدمة

تستهدف الباحثة من خلال هذا الجزء اختبار مدى مساهمة حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية. وذلك من خلال إجراء دراسة تجريبية استنادا إلى دراسات (على وعلى، 2022؛ شرف، 2023؛ Cheng et al., 2022 ;Badawy, 2021)، ولذلك يختص هذا الجزء بتحديد إجراءات الدراسة التجريبية، والتي تتضمن تحديد مجتمع وعينة الدراسة، وتصميم الدراسة التجريبية، وتوصيف متغيرات الدراسة، واختبار الفروض وتحليل ومناقشة النتائج.

6-3-2 مجتمع وعينة الدراسة

تمثل مجتمع الدراسة التجريبية في المحاسبين والمراجعين الداخليين العاملين بالبنوك المقيدة بالبورصة المصرية والبالغ عددها أحد عشر بنكًا، وقد تم اختيار عينة البحث بصورة تحكمية، والتي بلغ عددها 105 مفردة من المحاسبين (بمسميات وظيفية مختلفة) والمراجعين الداخليين بتلك البنوك. ويرجع اختيار عينة الدراسة بصورة تحكمية نظراً لظروف وطبيعة جمع بيانات الدراسة التجريبية، ويوضح الجدول رقم (3) التالي عدد القوائم الموزعة على عينة الدراسة، بالإضافة إلى عدد ونسبة الردود.

جدول 3: عينة الدراسة التجريبية وعدد ونسبة الردود

بيان	عدد القوائم الموزعة	عدد القوائم المستلمة	النسبة المؤية للردود المقبولة
المحاسبون (بمسميات وظيفية مختلفة)	54	54	%100
المراجعون الداخليون	51	51	%100
الإجمالى	**105**	**105**	**%100**

6-3-3 خصائص عينة الدراسة

في ضوء الردود التي تم الحصول عليها أمكن للباحثة توصيف مفردات عينة الدراسة على أساس عدد سنوات مزاولة المهنة، والمؤهل العلمي، وذلك كما يتضح من الجدول رقم (4) التالي:

جدول 4: خصائص عينة الدراسة

الخصائص	التكرارات	النسبة
المؤهل العلمي:		
بكالوريوس	69	65,71
ماجستير	19	18,10
دكتوراه	17	16,19
الإجمالى	105	**%100**
عدد سنوات مزاولة المهنة:		
أقل من 5 سنوات	10	9,52
من 5 الى 10 سنوات	25	23,81
أكثر من 10 سنوات	70	66,67
الإجمالى	105	**%100**

6-3-4 تصميم الدراسة التجريبية

تضمنت الدراسة التجريبية ثلاثة أقسام هي؛ **القسم الأول:** وقد تضمن الاستفسار عن بعض البيانات الديمغرافية للمشاركين في الدراسة كالاسم والمؤهل العلمي وعدد سنوات مزاولة المهنة. **القسم الثاني:** وقد تضمن تعريف لبعض المصطلحات ذات الصلة بموضوع الدراسة. **القسم الثالث:** وقد تضمن ثلاث حالات إفتراضية لأحد بنوك القطاع الخاص المقيدة ببورصة تداول الأوراق المالية المصرية، وذلك لاختبار فروض البحث. حيث تمثلت **الحالة الأولى** في افتراض أن البنك قد قرر العمل على تعزيز ثقافة الأمن السيبراني ورفع الوعي بمخاطر الهجمات الإلكترونية، وذلك من خلال اتخاذ العديد من التدابير والإجراءات لتفعيل حوكمة الأمن السيبراني، وذلك لمواجهة الهجمات الإلكترونية على نحو يضمن المنع أو التقليل من حدوثها إلى جانب سرعة التعافي من آثارها. وقد تم عرض تلك الحالة على المجموعة المشاركة في الدراسة، وذلك لاختبار مدى موافقة تلك المجموعة على إسهام تلك التدابير والإجراءات (ضوابط حوكمة الأمن السيبراني) بشكل إيجابي في الحد من مخاطر الهجمات الإلكترونية من خلال الرد على مجموعة من الأسئلة الموجهة لهم.

وتمثلت **الحالة الثانية** في افتراض وجود شكاوى من المستثمرين وغيرهم من أصحاب المصالح من عدم وجود معلومات كافية، وفي الوقت المناسب عن مخاطر الأمن السيبراني التي يتعرض لها البنك، وجهوده في إدارة تلك المخاطر. وبالتالي عدم قدرتهم على تقييم موقف الأمن السيبراني لديه، ومعرفة مدى فعالية برامجه في إدارة تلك المخاطر، خاصة وقد اهتم عدد من المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن مخاطر الأمن السيبراني وبرنامج إدارتها. وبناءا على ذلك فإن البنك قد قرر التخطيط للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن السيبراني. وذلك لاختبار مدى موافقة المجموعة المشاركة في الدراسة على إسهام تطبيق ضوابط حوكمة الأمن السيبراني بشكل إيجابي في تشجيع البنك على الإفصاح عن إدارة مخاطر الأمن السيبراني، باعتبار أن هذا التطبيق في حد ذاته، يمثل ذلك الجزء من الإفصاح الذي يعمل على بث إشارات إيجابية بشأن الجهود المبذولة من قبل المنشأة لتقليل مخاطر الأمن السيبراني أو الحد منها ومنعها، وذلك من خلال الرد على أحد الأسئلة الموجهة إليهم.

في حين تمثلت **الحالة الثالثة** والأخيرة في تصميم تقرير افتراضي عن إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن السيبراني بالبنك، لاختبار مدى موافقة المجموعة المشاركة في الدراسة على إسهام الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن

السيبراني بشكل إيجابي في تحسين الأداء المالي للبنك، وذلك من خلال الرد على مجموعة من الأسئلة الموجهة لهم.

6-3-5 توصيف متغيرات الدراسة

استنادا إلى ما تم عرضه من خلال مشكلة البحث، وأهدافه، وفروضه، يمكن تحديد وتوصيف متغيرات الدراسة على النحو التالي؛ **(أولا)** المتغير المستقل: الإفصاح عن إدارة مخاطر الأمن السيبراني. **(ثانيا)** المتغير التابع: الأداء المالي. **(ثالثا)**: المتغير المعدل: حوكمة الأمن السيبراني. وقد تم اختبار العلاقات بين تلك المتغيرات من خلال تقييم استجابات المستقصى منهم المشاركين في الدراسة على الأسئلة المرفقة بالحالات التجريبية (انظر ملحق رقم 1)، وذلك بالاعتماد على مقياس ليكرت ذي الخمس درجات، حيث يمكن تحديد اتجاه عينة الدراسة نحو رفض أو قبول الفروض في ضوء حساب المتوسط الحسابي، والذي تتراوح قيمته من 1 إلى 5 على مقياس ليكرت الخماسي، كما هو موضح بالجدول رقم (5) التالي:

جدول 5: اتجاه آراء عينة الدراسة في ضوء المتوسط الحسابي على مقياس ليكرت الخماسي

الدرجة	قيمة المتوسط الحسابي	الرأي
1	من 1 إلى 1,80	غير موافق بتاتاً
2	من 1,81 إلى 2,60	غير موافق
3	من 2,61 إلى 3,40	محايد
4	من 3,41 إلى 4,20	موافق
5	من 4,21 إلى 5	موافق تماماً

المصدر :(Nyutu 2021)

6-3-6 الأساليب الإحصائية المستخدمة

تم تشغيل بيانات الدراسة باستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، والتي تعد من أكثر البرامج الإحصائية شيوعاً واستخداما في مجال العلوم الاجتماعية. وذلك لتحليل بيانات الدراسة واختبار الفروض الخاصة بها، إعتماداً على مجموعة من الأساليب والاختبارات الإحصائية، والتي يمكن إيضاحها على النحو التالي:

6-3-6-1 أسلوب الإحصاء الوصفي

ويتمثل في كل من؛ التكرارات، والنسب المئوية، والمتوسط الحسابي، والوسيط، والانحراف المعياري، ومعامل الاختلاف.

6-3-6-2 أسلوب الإحصاء التحليلي

ويتمثل في كل من؛ **(أولا): معامل الثبات ألفا كرونباخ**[3] **Coronbach's Alpha** لقياس ثبات وصدق مدى الاتساق الداخلي بين إجابات كل سؤال مع الأسئلة الأخرى، ومن ثم إمكانية الإعتماد على البيانات المجمعة واستخدامها في التحليل الإحصائي. **(ثانيا): اختبار ويلكوكسن لعينة واحدة one-sample Wilcoxon signed rank test** والمعروف باختبار إشارات الرتب، والذي يستخدم لقياس معنوية الفروق بين قيمة الوسيط المحسوبة وفقا لآراء عينة الدراسة وقيمة الوسيط المفترضة لمجتمع الدراسة، والتي تمثل حالة الحياد للمستقصى منه، بحيث تكون فرضية الاختبار على النحو التالي:

فرض العدم: لا توجد فروق ذات دلالة إحصائية بين وسيطي العينة ومجتمع الدراسة

$$H_0 : \mu_1 = \mu_2$$

الفرض البديل: توجد فروق ذات دلالة إحصائية بين وسيطي العينة ومجتمع الدراسة

$$H_1 : \mu_1 \neq \mu_2$$

ووفقا لهذا الاختبار إذا كانت قيمة (P-Value) أقل من (5%) يرفض فرض العدم ويقبل الفرض البديل والعكس صحيح.

6-3-7 نتائج اختبار فروض الدراسة

6-3-7-1 نتائج اختبار الفرض الأول

استهدف الفرض الأول **(H_1) اختبار مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية**، ويوضح الجدول رقم (6) التالي مقاييس الإحصاء الوصفي لضوابط حوكمة الأمن السيبراني، وذلك لتحديد اتجاه آراء مفردات عينة الدراسة نحو قبول أو رفض مساهمة تلك الضوابط في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية.

[3] يمكن قبول معامل الثبات ألفا كرونباخ اذا كانت قيمته ≥ 0,6

جدول 6: مقاييس الإحصاء الوصفي للفرض الأول

م	ضوابط حوكمة الأمن السيبراني	عدد المشاهدات	المتوسط الحسابي	الوسيط	الانحراف المعياري	معامل الاختلاف
1	قيام مجلس إدارة البنك بتحديد وتوثيق واعتماد إستراتيجية للأمن السيبراني، وتنفيذ برنامج عمل لتطبيقها، ومراجعتها على فترات زمنية مخطط لها.	105	4,81	5,000	0,395	0,082
2	إنشاء إدارة معنية بالأمن السيبراني في البنك وأن تكون مستقلة عن إدارة تكنولوجيا المعلومات والاتصالات، مع تشكيل لجنة إشرافية للأمن السيبراني بتوجيه من مجلس الإدارة على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها.	105	4,77	5,000	0,422	0,088
3	قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات، وتوثيقها واعتمادها من مجلس الإدارة، ونشرها إلى ذوي العلاقة من العاملين في البنك والأطراف المعنية بها والعمل على ضمان تطبيقها، ومراجعتها على فترات زمنية مخطط لها.	105	4,76	5,000	0,428	0,09
4	قيام مجلس إدارة البنك بتحديد وتوثيق وإعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للبنك وتقديم الدعم اللازم لإنفاذ ذلك، مع مراجعة هذه الأدوار والمسئوليات وتحديثها على فترات زمنية مخطط لها.	105	4,75	5,000	0,434	0,091
5	قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني بالبنك وفقا لإعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية، وضمان العمل على تطبيقها ومراجعتها وتحديثها على فترات زمنية مخطط لها.	105	4,73	5,000	0,444	0,094
6	تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في البنك لضمان تحديد مخاطر الأمن السيبراني ومعالجتها	105	4,71	5,000	0,454	0,096

	كجزء من دورة حياة المشروع التقني ومراجعتها دوريا.					
7	إلتزام البنك بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني، وأي اتفاقيات أو التزامات دولية معتمدة محليا تتضمن متطلبات خاصة بالأمن السيبراني.	**105**	**4,73**	**5,000**	**0,444**	0,094
8	مراجعة تطبيق ضوابط الأمن السيبراني بالبنك دوريا، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني بشكل مستقل يراعى فيه عدم تعارض المصالح ووفقا للمعايير العامة المقبولة للمراجعة والتدقيق، مع توثيق نتائج عملية المراجعة.	**105**	**4,73**	**5,000**	**0,444**	0,094
9	تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند إنتهاء/إنهاء عملهم بالبنك.	**105**	**4,78**	**5,000**	**0,416**	0,087
10	تطوير واعتماد برنامج دورى للتوعية بالأمن السيبراني في البنك، والتأكد من تزويد العاملين بالبنك بالمهارات والدورات التدريبية المطلوبة في مجال الأمن السيبراني.	**105**	**4,79**	**5,000**	**0,409**	0,085
المتوسط العام		**105**	**4,758**	**5,000**	**0,341**	0,072

يتضح من خلال تحليل بيانات الجدول رقم (6) السابق أن آراء مفردات العينة قد أظهرت اتجاها عاما نحو الموافقة التامة على مساهمة ضوابط حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية، وذلك بمتوسط حسابي مقداره (4,758)، وبمعامل اختلاف معياري مقداره (0,072).

وقد بلغ معامل الثبات ألفاكرونباخ لإجمالى عبارات الفرض الأول (0,935) وهو ما يدل على ثبات وصدق مدى الاتساق الداخلي بين إجابات كل عبارة مع العبارات الأخرى، ومن ثم يمكن الإعتماد على البيانات المجمعة واستخدمها في التحليل الإحصائي، ويوضح الجدول رقم (7) التالي اختبار ويلكوكسن لعينة واحدة Wilcoxon signed rank test one-sample لقياس معنوية الفروق بين قيمة الوسيط المحسوبة وفقا لآراء عينة الدراسة، وقيمة الوسيط المفترضة لمجتمع الدراسة وهى 3 (محايد) على مقياس ليكرت الخماسي، وذلك لتحديد مدى قبول أو رفض الفرض الأول.

جدول 7: نتائج اختبار Wilcoxon signed rank للفرض الأول

Ranks			
Sign	**Obs**	**Rank**	**Expected**
Positive Ranks	105	5565	2782.5
Negative Ranks	0	0	2782.5
	105	5565	5565
Test Statistics			
Z	9.064		
Prob > |z|	0.000		

*** p<0.01, ** p<0.05, * p<0.1

ويتضح من الجدول رقم (7) السابق تركز إجابات مفردات عينة الدراسة في الرتب الموجبة Positive Ranks، مما يشير إلى اتجاه آراء العينة نحو الموافقة على أن تطبيق ضوابط حوكمة الأمن السيبراني يمكن أن يساهم ايجابيًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية.

كما أنه بناءا على قيمة Z والتي بلغت (9,064)، ومستوى المعنوية الذي بلغ (0,000)، فإنه توجد اختلافات ذات دلالة معنوية بين اتجاهات مفردات عينة الدراسة ومعلمة مجتمع الدراسة نحو مدى مساهمة ضوابط حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية عند مستوى معنوية أقل من (1%). مما يشير إلى **رفض فرض العدم الإحصائي** والذي يقضي بأن آراء عينة الدراسة تميل نحو الحياد، **وقبول الفرض الإحصائي البديل** والذي يؤيد اتجاه آراء مفردات العينة نحو الموافقة على مساهمة ضوابط حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية، ومن ثم قبول الفرض الأول.

6-3-7-2 نتائج اختبار الفرض الثاني

استهدف الفرض الثاني **(H_2) اختبار مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية**، ويوضح الجدول رقم (7) التالي مقاييس الإحصاء لمدى مساهمة حوكمة الأمن السيبراني في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وذلك لتحديد اتجاه آراء مفردات عينة الدراسة نحو قبول أو رفض هذا الفرض.

جدول 8: مقاييس الإحصاء الوصفي للفرض الثاني

التساؤل البحثى	عدد المشاهدات	المتوسط الحسابي	الوسيط	الانحراف المعياري	معامل الاختلاف
هل يسهم تطبيق ضوابط حوكمة الأمن السيبراني في تشجيع البنك على الإفصاح عن إدارة مخاطر الأمن السيبراني، باعتبار أن هذا التطبيق في حد ذاته، يمثل ذلك الجزء من الإفصاح الذي يعمل على بث إشارات إيجابية بشأن الجهود المبذولة من قبل المنشأة لتقليل مخاطر الأمن السيبراني أو الحد منها ومنعها.	**105**	**4,81**	**5,000**	**0,395**	0,082

يتضح من خلال تحليل بيانات الجدول رقم (8) السابق أن آراء مفردات العينة قد أظهرت اتجاها عاما نحو الموافقة التامة على مساهمة تطبيق ضوابط حوكمة الأمن السيبراني ايجابيًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية، وذلك بمتوسط حسابي مقداره (4,81)، وبمعامل اختلاف معياري مقداره (0,082).

ويوضح الجدول رقم (9) التالي اختبار ويلكوكسن لعينة واحدة Wilcoxon signed one-sample rank test لقياس معنوية الفروق بين قيمة الوسيط المحسوبة وفقا لآراء عينة الدراسة، وقيمة الوسيط لمجتمع الدراسة وهى 3 (محايد) على مقياس ليكرت الخماسي، وذلك لتحديد مدى الموافقة على قبول أو رفض الفرض الثاني.

جدول 9: نتائج اختبار Wilcoxon signed rank للفرض الثاني

Ranks			
Sign	**Obs**	**Rank**	**Expected**
Positive Ranks	105	5565	2782.5
Negative Ranks	0	0	2782.5
	105	5565	5565
Test Statistics			
Z	9.555		
Prob > |z|	0.000		

*** p<0.01, ** p<0.05, * p<0.1

ويتضح من الجدول رقم (7) السابق تركز إجابات مفردات عينة الدراسة في الرتب الموجبة Positive Ranks، مما يشير إلى اتجاه آراء العينة نحو الموافقة على أن تطبيق ضوابط حوكمة الأمن السيبراني يمكن أن يساهم ايجابيًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية.

كما أنه بناءا على قيمة Z والتي بلغت (9,555)، ومستوى المعنوية الذي بلغ (0,000)، فإنه توجد اختلافات ذات دلالة إحصائية بين اتجاهات مفردات عينة الدراسة ومعلمة مجتمع الدراسة نحو مدى مساهمة تطبيق ضوابط حوكمة الأمن السيبراني في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية، عند مستوى معنوية أقل من (1%). مما يشير إلى **رفض فرض العدم الإحصائي** والذي يقضى بأن آراء عينة الدراسة تميل نحو الحياد، **وقبول الفرض الإحصائي البديل** والذي يؤيد اتجاه آراء عينة الدراسة نحو الموافقة على مساهمة تطبيق ضوابط حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية، ومن ثم قبول الفرض الثاني.

6-3-7-3 نتائج اختبار الفرض الثالث

استهدف الفرض الثالث **(H_3) اختبار ما إذا كان الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني يسهم ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية**، ويوضح الجدول رقم (10) التالي مقاييس الإحصاء الوصفي لمدى مساهمة الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية، وذلك لتحديد اتجاه آراء مفردات عينة الدراسة نحو قبول أو رفض هذا الفرض.

جدول 10: مقاييس الإحصاء الوصفي للفرض الثالث

م	منافع الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني لتحسين الأداء المالي	عدد المشاهدات	المتوسط الحسابي	الوسيط	الانحراف المعياري	معامل الاختلاف
1	الحفاظ على سمعة البنك وزيادة ثقة المتعاملين معه مما يسهم في تحسين الأداء المالي للبنك.	105	4,859	5,000	0,308	0,063
2	زيادة ملائمة وموثوقية المعلومات المالية، مما يؤدي إلى جذب مزيد من العملاء وتحقيق قدر أكبر من العوائد.	105	4,905	5,000	0,295	0,060
3	زيادة رضاء العملاء الحاليين وجذب مزيد من العملاء المستقبليين.	105	4,886	5,000	0,320	0,065
4	الحد من الغش والتلاعب المالي الإلكتروني ، مما ينعكس بالإيجاب على كفاءة الأداء المالي للبنك	105	4,886	5,000	0,320	0,065
5	رفع كفاءة نظم الرقابة والمراجعة الداخلية وتحسين قدرتها على متابعة وتقييم ضوابط الأمن السيبراني لحماية أمن المعلومات المالية، مما يسهم في تحسين الأداء المالي للبنك.	105	4,905	5,000	0,295	0,060

6	تمكين العملاء وغيرهم من أصحاب المصالح من تقييم قدرة البنك على التصدي للتهديدات السيبرانية ومعالجتها، ومن ثم تعزيز الثقة في الخدمات المصرفية المقدمة، وهو ما يعمل بدوره على جذب مزيد من العملاء، ومن ثم زيادة المدخرات وإرتفاع نسب السيولة لدى البنك وبالتالي تحسين أدائه المالي.	**105**	**4,924**	**5,000**	**0,267**	**0,054**
المتوسط العام		**105**	**4,9**	**5,000**	**0,222**	**0,045**

يتضح من خلال تحليل بيانات الجدول رقم (10) السابق أن آراء مفردات العينة قد أظهرت اتجاها عاما نحو الموافقة التامة على أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني من المتوقع أن يسهم ايجابيًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية، وذلك بمتوسط حسابي مقداره (4,9)، وبمعامل اختلاف معياري مقداره (0,045).

وقد بلغ معامل الثبات ألفاكرونباخ لإجمالي عبارات الفرض الثالث (0,833) وهو ما يدل على ثبات وصدق مدى الاتساق الداخلي بين إجابات كل عبارة مع العبارات الأخرى، ومن ثم يمكن الإعتماد على البيانات المجمعة واستخدمها في التحليل الإحصائي، ويوضح الجدول رقم (11) التالي اختبار ويلكوكسن لعينة واحدة Wilcoxon signed rank test one-sample لقياس معنوية الفروق بين قيمة الوسيط المحسوبة وفقا لآراء عينة الدراسة، وقيمة الوسيط لمجتمع الدراسة وهى 3 (محايد) على مقياس ليكرت الخماسي، وذلك لتحديد مدى الموافقة على قبول أو رفض الفرض الثاني.

جدول 11: نتائج اختبار Wilcoxon signed rank للفرض الثالث

Ranks			
Sign	**Obs**	**Rank**	**Expected**
Positive Ranks	105	5565	2782.5
Negative Ranks	0	0	2782.5
	105	5565	5565
Test Statistics			
Z	9.314		
Prob > |z|	0.000		

*** p<0.01, ** p<0.05, * p<0.1

ويتضح من الجدول رقم (11) السابق تركز إجابات مفردات عينة الدراسة في الرتب الموجبة Ranks Positive، مما يشير إلى اتجاه آراء العينة نحو الموافقة على أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني من المتوقع أن يسهم ايجابيًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

كما أنه بناءا على قيمة Z والتي بلغت (9,314)، ومستوى المعنوية الذي بلغ (0,000)، فإنه توجد اختلافات ذات دلالة إحصائية بين اتجاهات مفردات عينة الدراسة ومعلمة مجتمع الدراسة نحو مدى مساهمة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية عند مستوى معنوية أقل من (1%). مما يشير إلى **رفض فرض العدم الإحصائي** والذي يقضى بأن آراء عينة الدراسة تميل نحو الحياد، **وقبول الفرض الإحصائي البديل** والذي يؤيد اتجاه آراء مفردات عينة الدراسة نحو الموافقة على أن الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني يمكن أن يسهم ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية، ومن ثم قبول الفرض الثالث.

6-4 خلاصة البحث ونتائجه والتوصيات ومقترحات الأبحاث المستقبلية

6-4-1 خلاصة البحث ونتائجه

تمثل الهدف الرئيس لهذا البحث في اختبار مدى مساهمة تطبيق حوكمة الأمن السيبراني في الحد من مخاطر الهجمات الإلكترونية بالبنوك كمدخل لتفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، وانعكاس ذلك على تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية. ولتحقيق هذا الهدف قامت الباحثة بتناول عدة جوانب هى؛ أولا: الإطار المفاهيمي للبحث، ثانيا: الدراسات السابقة وإشتقاق فروض البحث، ثالثا: الدراسة التجريبية، وقد توصلت الباحثة من خلال دراستها النظرية والتطبيقية إلى مجموعة من النتائج يمكن إيجاز أهمها في الآتي:

- شهدت السنوات القليلة الماضية زيادة كبيرة في عدد الهجمات الإلكترونية التي تستهدف القطاع المصرفي في مختلف دول العالم، حتى أصبحت تلك الهجمات تشكل خامس أكبر تهديد للاقتصاد العالمي.
- الهجمات الإلكترونية هى عمليات تستهدف اختراق نظم المعلومات الرقمية الخاصة بالأفراد أو المؤسسات بهدف سرقتها أو التعديل عليها أو إتلافها لأغراض إجرامية مختلفة، وذلك بالاعتماد على البرامج والتقنيات الحديثة في مجال تكنولوجيا المعلومات.
- تؤثر الهجمات الإلكترونية على الجوانب الرئيسية لأمن المعلومات والتي تتمثل في سرية ونزاهة وتوافر المعلومات، مما يكبد المؤسسات المالية خسائر مالية فادحة قد تصل بها إلى حد الانهيار، وتكمن خطورتها في اعتمادها على تقنيات حديثة ومتطورة، فضلا عن سهولة وسرعة انتشارها، إلى جانب اتساع نطاق تأثيرها في وقت قصير وعن بعد.

- احتلت قضية الأمن السيبراني اهتمام الساحة الاقتصادية العالمية، وذلك في ظل التطور الراهن في مجال تكنولوجيا المعلومات والإتصالات وتسارع خطى المؤسسات وبصفة خاصة المالية نحو تبنى إستراتيجيات التحول الرقمي، وذلك باعتبار أن الأمن السيبراني يعد أحد أهم الركائز الأساسية لمواجهة مخاطر الهجمات الإلكترونية.
- أصبح تعزيز قدرات البنوك وأمنها السيبراني في مواجهة الهجمات الإلكترونية أمرا حتميا وذلك في ظل التحول نحو الصيرفة الرقمية والتوسع في تقديم الخدمات والمنتجات الإلكترونية.
- الأمن السيبراني هو عملية مستمرة لتأمين الأنظمة المتصلة بشبكة الإنترنت متضمنة الأجهزة والبرامج والبيانات من الهجمات الإلكترونية والتعافي منها حال حدوثها، وذلك على نحو يضمن الحفاظ على سرية البيانات وسلامتها وتوافرها.
- تأتى حوكمة الأمن السيبراني على رأس الضوابط الأساسية للأمن السيبراني والتي يمكن تعريفها بأنها مجموعة من أفضل الممارسات التي تضبط وتوجه أعمال المنشأة فيما يتعلق بتعزيز الأمن السيبراني، وتحقيق المرونة السيبرانية في مواجهة الهجمات الإلكترونية على نحو يضمن المنع أو التقليل من حدوثها إلى جانب سرعة التعافي من آثارها.
- ازدادت شكاوى العملاء والمستثمرين وغيرهم من أصحاب المصالح من عدم وجود معلومات كافية وفي الوقت المناسب عن مخاطر الأمن السيبراني التي تتعرض لها منشآت الأعمال وجهودها في إدارة تلك المخاطر، وبالتالي عدم قدرتهم على تقييم موقف الأمن السيبراني لها ومدى فعالية برامجها في إدارة مخاطر الأمن السيبراني.
- اهتمت المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن جهودها في مجال الأمن السيبراني من خلال إعداد تقرير إدارة مخاطر الأمن السيبراني، ويأتي في مقدمتها الإرشادات الصادرة عن هيئة الأوراق المالية والبورصات الأمريكية (SEC)، والمعهد الأمريكي للمحاسبين القانونيين .(AICPA)
- تباينت الآراء ما بين مؤيد ومعارض لجدوى الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وعلاقته بالأداء المالي لمنشآت الأعمال بصفة عامة والبنوك بصفة خاصة، وذلك باعتبار أن البنوك من أكثر منشآت الأعمال استهدافا بالهجمات الإلكترونية.

- أكدت نتائج التحليل الإحصائي اتجاه آراء مفردات عينة الدراسة نحو الموافقة التامة على مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في الحد من مخاطر الهجمات الإلكترونية بالبنوك المقيدة بالبورصة المصرية.

- أكدت نتائج التحليل الإحصائي اتجاه آراء مفردات عينة الدراسة نحو الموافقة التامة على مساهمة حوكمة الأمن السيبراني ايجابيًا ومعنويًا في تفعيل الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني بالبنوك المقيدة بالبورصة المصرية.

- أكدت نتائج التحليل الإحصائي اتجاه آراء مفردات عينة الدراسة نحو الموافقة التامة على أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل حوكمة الأمن السيبراني من المتوقع أن يسهم ايجابيًا ومعنويًا في تحسين الأداء المالي بالبنوك المقيدة بالبورصة المصرية.

6-4-2 التوصيات

في ضوء النتائج التي أسفرت عنها هذه الدراسة، توصي الباحثة بالآتى:

- ضرورة قيام الهيئة العامة للرقابة المالية بالتعاون مع القطاع المصرفي المصري بتوفير دورات تدريبية عالية المستوى، وتنظيم ندوات ومؤتمرات في مجال تعزيز الأمن السيبراني وتطبيق ضوابط حوكمة الأمن السيبراني بالبنوك، لخلق كوادر قادرة على مواجهة التحديات السيبرانية وعلى رأسها الهجمات الإلكترونية.

- ضرورة قيام الأجهزة الرقابية بالدولة والمعنية بالقطاع المصرفي بوضع آليات رقابية واضحة للتأكد من التزام البنوك بتطبيق ضوابط الأمن السيبراني وفي مقدمتها حوكمة الأمن السيبراني ، والإفصاح عن تقرير إدارة مخاطر الأمن السيبراني.

- ضرورة قيام البنوك المصرية بالعمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع مستوى الوعي بقضايا الأمن السيبراني.

- يجب دعم وتعزيز المهارات الرقمية للموارد البشرية العاملة بالبنوك وبصفة خاصة المراجعيين الداخليين لضمان كفاءة وفعالية التعامل مع مخاطر الهجمات الإلكترونية، وذلك من خلال توفير الدورات التدريبية وورش العمل ذات الصلة بإدارة مخاطر الأمن السيبراني.

- ضرورة تضمين المقررات الدراسية المخصصة لمرحلتي البكالوريوس والدراسات العليا مقرر يختص بالأمن السيبراني في القطاع المصرفي وإدارة مخاطره.

- ضرورة قيام مجلس معايير المحاسبة الدولية IASB بإصدار معيار دولي يعمل على تنظيم جوانب المراجعة والتدقيق فيما يتعلق بالأمن السيبراني وإصدار تقرير مستقل للمراجع لتأكيد إدارة مخاطر الأمن السيبراني.
- ضرورة قيام الباحثين بإجراء المزيد من الدراسات التي من شأنها تقديم تفسيرات إضافية للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وتطبيق حوكمة الأمن السيبراني بالبنوك لتحسين أدائها المالي ودعم قدرتها التنافسية.

6-4-3 مقترحات الأبحاث المستقبلية

في ضوء النتائج التي توصلت إليها الباحثة، فإنها تقترح بعض المجالات التي يمكن أن تشكل أفكارا لبحوث مستقبلية، والتي يمكن إيضاحها على النحو التالي:

- أثر الثقة الإدارية المفرطة على نغمة الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وانعكاس ذلك على قيمة المنشأة.
- أثر جودة المراجعة الداخلية على تفعيل ضوابط حوكمة الأمن السيبراني وانعكاس ذلك على جودة المعلومات المحاسبية.
- أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على ميول المستثمرين وانعكاس ذلك على كفاءة الاستثمار.
- مدخل مقترح لتأكيد تقرير إدارة مخاطر الأمن السيبراني وانعكاس ذلك على قرارات المستثمرين.
- أثر الإفصاح عن إدارة مخاطر الأمن السيبراني على خطر انهيار أسعار الأسهم.

المراجع

أولاً: المراجع باللغة العربية

أبو الخير، محمد حارس محمد طه (2022). أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية: دراسة ميدانية. ***المجلة العلمية للدراسات والبحوث المالية والتجارية***. العدد الأول، المجلد (15): 1 – 65.

أبو زيد. عبد الرحمن عاطف. الأمن السيبراني في الوطن العربى: دراسة حالة المملكة العربية السعودية. ***مجلة المركز العربى للبحوث والدراسات***. العدد (48): 55 – 61.

أبو سمك، أحمد محمد علي (2023). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على استجابة أسعار الأسهم للإعلان عن الأرباح: أدلة تطبيقية من البنوك المصرية المدرجة. ***المجلة العلمية للدراسات المحاسبية***. العدد الرابع، المجلد(5): 288 – 351.

أحمد، خالد محمد عثمان (2023). أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي :دراسة تطبيقية. ***مجلة البحوث المحاسبية***.العدد الرابع: 1107 – 1183.

أحمد، راميار رازكار (2021). دور نظام المعلومات المحاسبية الإلكتروني في تعزيز أمن المعلومات المالية. **المجلة الدولية للعلوم الإنسانية والاجتماعية** . العدد 24 (سبتمبر 2021): 254 – 282.

إسماعيل، أيمن محمد (2020). تأثير الهجمات الإلكترونية على فاعلية النظام الإيكولوجى الرقمي. ***مجلة مصر المعاصرة***. المجلد 111، العدد (540): 581 – 620.

إسماعيل، محمد (2019). الأمن السيبراني في القطاع المصرفي. ***صندوق النقد العربى***. موجز سياسات: العدد الرابع (يونيو 2019): 1 – 8. متاح على: https://www.amf.org.ae

الإستراتيجية الوطنية للأمن السيبراني (2017 – 2021). 2018. مصر. متاح على: https://mcit.gov.eg

الأمير، شمران عبيد خليف (2022). أثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني. ***مجلة الكويت للعلوم الاقتصادية والإدارية***. العدد الرابع عشر، المجلد (45): 486 – 503.

البوابة الإلكترونية لدولة الإمارات (2022). الأمن السيبراني والسلامة. متاح على: https://u.ae

الرشيدى، طارق عبد العظيم؛ عباس، داليا عادل (2019). أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات. ***مجلة المحاسبة والمراجعة***. العدد الثاني، المجلد (8): 439 – 487.

السمحانى، منى عبد الله (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. ***مجلة كلية التربية – جامعة المنصورة***. العدد 111، المجلد (1):3 – 31.

الهيئة الوطنية للأمن السيبراني – المملكة العربية السعودية (2018). الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018). متاح على: https://nca.gov.sa

جمال، زمورة؛ بن عيسى، ليلى(2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر. ***مجلة البحوث الاقتصادية المتقدمة***.العدد الثاني، المجلد (7):414–429.

حامد، خليل محمد؛ إبراهيم، عماد الدين؛ عبد الجليل، محمد حسن. جودة المعلومات المحاسبية وأثرها في تحسين الأداء المالي: دراسة ميدانية على سوق الخرطوم للأوراق المالية. ***مجلة جامعة أم درمان الإسلامية***. العدد (33): 26 – 51.

خشبة، محمد ماجد؛ الريس، أمانى حلمى؛ الجوهرى، عصام محمد؛ ابراهيم، داليا أحمد؛ العزب، هبة جمال؛ حسن، حسن محمد (2021). الأبعاد التنموية والإستراتيجية للأمن السيبراني ودوره في دعم الاقتصاديات الرقمية والمشفرة – مسارات التجربة المصرية في ضوء التجارب العالمية. ***سلسلة قضايا التخطيط والتنمية رقم (326) – معهد التخطيط القومى***. الطبعة الأولى (2021): 1 – 206.

شرف، أحمد إبراهيم (2023). إثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين: دراسة تجريبية. ***مجلة الإسكندرية للبحوث المحاسبية***. العدد الأول، المجلد (7): 211 – 281.

طارق، عامر ؛ الإتربى، محمد صبحى؛ فتوح، وسام حسن؛ ألفارس عبد المحسن؛ فودة، خالد (2021). إنشاء مركز متخصص ومتكامل للأمن السيبراني ليصبح أول المراكز القطاعية من نوعها في مصر – الملتقى المصرفي العربي الأول للأمن السيبراني في شرم الشيخ: نظمه اتحاد المصارف العربية تحت رعاية محافظ البنك المركزي المصري. ***مجلة إتحاد المصارف العربية***. العدد (491): 6 – 29.

على، محمود أحمد أحمد؛ و علي، صالح علي صالح (2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن لسيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية :دراسة تجريبية. ***مجلة الإسكندرية للبحوث المحاسبية***. العدد الثالث، المجلد (6): 1 – 48.

قاسم، زينب عبد الحفيظ؛ رشوان، عبد الرحمن محمد (2022). أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك. ***المؤتمر العلمي الدولي الأول بعنوان " أثر الأمن السيبراني على الأمن الوطني "***. جامعة عمان العربية: 1 – 29.

محمد، حسناء عطية حامد (2023). المقدرة التقيمية للافصاح عن ضوابط حوكمة الامن السيبراني وتأثيره على قرارات المستثمرين :دراسة تطبيقية على شركتى الاتصالات السعودية (زين –STC). المجلة المصرية للدراسات التجارية. العدد الرابع، المجلد (47): 1 – 54.

نصار. ولاء محمد الطاره عبد الخالق (2021). آليات مركز دبى للأمن الإلكتروني للتوعية بالإستراتيجيات الوطنية للأمن السيبراني للحكومات الذكية عبر منصات التواصل الإجتماعى. ***مجلة إتحاد الجامعات العربية لبحوث الإعلام وتكنولوجيا الإتصال***. العدد (6): 46 – 108.

يوسف، أماني أحمد وهبة (2022). واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة: دراسة تطبيقية. ***المجلة العلمية للدراسات التجارية والبيئية***. العدد الثاني، المجلد (13): 28 – 109.

ثانياً: المراجع باللغة الأجنبية

AICPA (American Institute of Certified Public Accountants) (2017). Cybersecurity risk management reporting Framework. Available at: https://www.aicpa.org/news/article/aicpa-unveils-cybersecurity-risk-management-reporting-framework.

Akinbowale, O. E., H. E. Klingelhofer and M. F. Zerihun. 2020. Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. ***Journal of Financial Crime***. 27(3): 945 – 958.

Ali, S. M.; S. M. N. Hoq; A. B. M. M. Bari; G. Kabir and S. K. Paul (2022). Evaluating factors contributing to the failure of information system in the banking industry. ***PLoS ONE***. 17(3): 1 – 21.

Alina, C. M. (2017). Internal audit role in cybersecurity. ***Economic Sciences Series***. (XVII) 2: 510 -513.

Al-Tahat, S. and O. Abdel Moneim. (2020). The Impact Of Artificial Intelligence On The Correct Application Of Cyber Governance In Jordanian Commercial Banks. I***nternational Journal of Scientific & Technology Research***.9(3): 7138 – 7144.

Antoine, B. (2018). Cyber Risk for the financial sector: A Framework for Quantitative assessment. ***International Monetary Fund (IMF) working paper***. Available at: https://www.imf.org.

Ayuba, H., A. J. Bambale, M. A. Ibrahim and S. A. Sulaiman (2019). Effects of Financial Performance, Capital Structure and Firm Size on Firms' Value of Insurance Companies in Nigeria. Journal of Finance, Accounting and Management, 10(1): 57 – 74.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. ***Procedia Economics and Finance***. 28(2015): 24 – 31.

Berkman, H., J. Jona, G. Lee and N. Soderstrom (2018). Cybersecurity awareness and market valuations. ***Journal of Accounting and Public Policy***. 37 (6): 508-526.

Bongiovanni, I; K. Renaud; H. Brydon; R. Blignaut and A. Cavallo (2022). Evaluating factors contributing to the failure of information system in the banking industry. ***Information & Computer Security***. 30 (4): 517 – 548.

Bukht, T. F. N; R. Ahmed and J. Awan (2020). Analyzing cyber-attacks targeted on the banks of Pakistan and their solutions. ***International Journal of Computer Science and Network Security***. 20(2): 31 – 38.

Canelon, J.; E. Huerta; N. Leal and T. Ryan (2020). Unstructured Data for Cybersecurity and Internal Control. ***The 53rd Hawaii International Conference on System Sciences***. Available at: https://aisel.aisnet.org.

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

Cheong, A., K. Yoon, S. Cho and W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. ***Journal of information Systems***. 35 (2): 179-194.

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

CIS (Center for Internet Security) (2021). Breaking the Divide between Governance and Operational Cybersecurity. Available at: https://www.cisecurity.org/insights/blog/breaking-the-divide-between-governance-and-operational-cybersecurity.

De Matos, S. L. (2019). How Cyber governance Influences Relationships between companies. Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management, Universidade Nova de Lisboa. Available at: https://www.google. com/url?sa=t&source=web&rct=j&opi=89978449&url=https://run.unl.pt/bitstream/10362/99609/1/TGI0329.pdf&ved=2ahUKEwiS0OPGl6KIAxUBUKQEHSWBLrUQFnoECBMQAQ&usg=AOvVaw077cj4zOjOt9SMeS0ZB2kG.

Elnagar,S. M. A., A. S. A. Ahmed and M. M. M. Basiouny (2024). The impact of cybersecurity risk disclosure on the quality of financial reporting and market value. Evidence from Egyptian stock market. ***Educational Administration: Theory and Practice***. 30(5): 2504 - 2516.

Ettredge, M., G. Feng and L. Yijun (2018). Trade Secrets and Cybersecurity Breaches. ***Journal of Accounting and Public Policy***. 37(6): 564 – 585.

Frank, M. L., J. H. Grenier and J. S. Pyzoha (2019). How disclosing a prior cyber-attack influences the efficacy of cybersecurity risk management reporting and independent assurance. ***Journal of Information Systems***. 33 (3): 183-200.

Gatzert, N. and M. Schubert (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.

Goel, S. and H. A. Goel and Shawky (2014). The Impact of Federal and State Notification Laws on Security Breach Announcements. ***Communications of the Association for Information Systems***. 34(3): 37 – 50.

Hartmann C.C. and J. Carmenate (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. ***Current Issues in Auditing***.15 (2): 9 – 23.

Hathaway, O. A.; R. Crootof; P. Levitz; H. Nix; A. Nowlan; W. Perdue and J. Spiegel (2012). The Law of Cyber – Attack. ***California Law Review***. 100(4): 817 – 886.

ISO (2012). ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity.

ITU (The International Telecommunication Union) (2021). Global cybersecurity Index 2020. ITU publications. Available at: https://www.itu.int.

Kelton, A. S. and R. R. Pennington. 2020. Do voluntary disclosures mitigate the cybersecurity breach contagion effect? ***Journal of Information Systems***. 34 (3): 133–157.

Lagarde, C. (2018). Estimating Cyber Risk for the Financial Sector. ***IMF BLoG***. Available at: https://www.imf.org.

Li, H., W. G. No and T. Wang (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. ***International Journal of Accounting Information Systems***. 30(c): 40–55.

Maleh, Y.; A. Sahid and M. Belaissaow (2021). A maturity framework for cybersecurity governance in organizations. ***The EDP Audit, Control, and Security Newsletter (EDPACS)***. 63(6): 1 – 22.

Mazumder, M. M. M. and D. M. Hossain (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? ***Journal of Accounting in Emerging Economies***. April (2022): 1 – 23.

Meiryani, S. Huang, G. Soepriyanto, M. Fahlevi, S. Grabowska and M. Aljuaid. (2023).The effect of voluntary disclosure on financial performance: Empirical study on manufacturing industry in Indonesia. ***PLOS ONE***. 18(6): 1- 27.

Mijwil, M. M., Y. Filali, M. Aljanabi, M. Bounabi, H. Al-Shahwani and Chat GPT (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. ***Mesopotamian journal of Cybersecurity***. 2023: 1-6.

NCSC (National Cyber Security Centre) (2021). Cybersecurity Governance. Available at: https://www.ncsc.gov.uk.

Nyutu, E. N., W. W. Cobern and B. Pleasants (2021). Correlational study of student perceptions of their undergraduate laboratory environment with respect to gender and major. ***International Journal of Education in Mathematics, Science, and Technology (IJEMST)***. 9(1): 83-102.

Oladapo, I. A.; M. M. Hamoudah; M. Alam; O. R. Olaopa and R. Muda (2021). Customers' perceptions of FinTech adaptability in the Islamic banking sector: comparative study on Malaysia and Saudi Arabia. ***Journal of Modelling in Management***. 17 (4): 1241 – 1261.

Panda, A. and A. Bower (2020). Cyber security and the disaster resilience framework. ***International Journal of Disaster Resilience in the Built Environment***. 11(4): 507-518.

Potter, L. E. and Vickers, G. (2015). What Skills do you need to Work in Cyber Security? A Look at the Australian Markets. ***The 2015 ACM SIGMIS Conference on Computers and People Research***. Available at: https://research-repository.griffith.edu.au.

Pullin, D. (2018). Cybersecurity: positive changes through processes and team culture. ***Frontiers of Health Services Management***. 35(1): 3 – 12.

Qasaimeh, G. M. and H. E. Jaradeh (2022). The impact of artificial intelligence on the effective applying of cyber governance in Jordanian commercial banks. ***International Journal of Technology, Innovation and Management (IJTIM)***. 2(1): 68 – 86.

Roscini, M. (2010). World Wide Warfare - Jus ad bellum and the Use of Cyber Force. ***Max Planck Yearbook of United Nations Law***. (14) 2010:85 – 130.

Securities and Exchange Commission (SEC). (2011). CF disclosure guidance. Available at: https://www.sec.gov.

Securities and Exchange Commission (SEC). (2018). Commission statement and guidance on public company cybersecurity disclosures. Available at: https://www.sec.gov.

Securities and Exchange Commission (SEC). (2022). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Available at: https://www.sec.gov/corpfin/secg-cybersecurity.

Skinner, C. P. 2019. Bank Disclosures of Cyber Exposure. ***Lowa Law Review***. 105(2019): 239 – 281.

Solms, B. V. and R. V. Solms (2018). Sybersecurity and information security – what goes where? ***Information and computer security***. 26(1): 2 – 9.

Stanikzai, A. Q. and M. A. Shah (2021). Evaluation of Cyber Security Threats in Banking Systems. ***Conference: IEEE Symposium Series on Computational Intelligence (SSCI)***. Available at: https://ieeexplore.ieee.org.

Sullivan & Cromwell LLP. (2022). SEC Proposes New Cybersecurity Disclosure Rules for Public Companies. Available at: https://www.sullcrom.com.

Talal Albalas, T., A. Modjtahedi and R. Abdi. (2022). Cybersecurity governance: a scoping review. ***International Journal of Professional Business Review***. 7(4): 1 -19.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. ***International Review of Financial Analysis***. 76(July): 1-15.

Tudose, M. B. V. D. Rusu and S. Avasilcai. (2022).Financial performance – determinants and interdependencies between measurement indicators. ***Business, Management and Economics Engineering***. 20(1): 119 – 138.

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

World Bank. (2018). Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision. Available at: www.worldbank.org.

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

Yusif, S. and A. H. Baig. (2021). A Conceptual Model for Cybersecurity Governance. ***Journal of Applied Security Research***. 16(4): 1 – 24.

ملاحق البحث

ملحق 1: الضوابط الرئيسية لحوكمة الأمن السيبراني

م	الضوابط	التفسير
1	**إستراتيجة الأمن السيبراني**	- يجب على مجلس إدارة المنشأة تحديد وتوثيق واعتماد إستراتيجية للأمن السيبراني، وأن تتماشى هذه الإستراتيجية مع الإستراتيجية العامة للمنشأة والمتطلبات التشريعية والتنظيمية ذات الصلة، كما يجب العمل على تنفيذ برنامج عمل لتطبيق إستراتيجية الأمن السيبراني من قبل إدارة المنشأة، ويجب أيضا مراجعة هذه الإستراتيجية على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.
2	**إدارة الأمن السيبراني**	- يجب إنشاء إدارة معنية بالأمن السيبراني في المنشأة، وأن تكون مستقلة عن إدارة تقنية المعلومات والإتصالات، ويفضل ارتباطها مباشرة برئيس المنشأة أو من ينوبه، مع الأخذ في الاعتبار عدم تعارض المصالح. ويجب أن يشغل رئاسة هذه الإدارة والوظائف الإشرافية بها موظفين ذو كفاءة في مجال الأمن السيبراني. - كما يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من مجلس الإدارة لضمان التزام ودعم ومتابعة تطبيق برامج وسياسات الأمن السيبراني، على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها.
3	**سياسات وإجراءات الأمن السيبراني**	- يجب على الإدارة المعنية بالأمن السيبراني في المنشأة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات، وتوثيقها واعتمادها من مجلس الإدارة، ونشرها إلى ذوي العلاقة من العاملين في المنشأة والأطراف المعنية بها والعمل على ضمان تطبيقها. - ويجب أن تكون هذه السياسات والإجراءات مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات وأنظمة التشغيل وغيرها). - ويجب مراجعة هذه السياسات والإجراءات على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.
4	**أدوار ومسئوليات الأمن السيبراني**	- يجب على مجلس الإدارة تحديد وتوثيق وإعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للمنشأة، وتكليف الأشخاص المعنيين بها، وتقديم الدعم اللازم لإنفاذ ذلك، مع مراجعة هذه الأدوار والمسئوليات وتحديثها على فترات زمنية مخطط لها.
5	**إدارة مخاطر الأمن السيبراني**	- يجب على الإدارة المعنية بالأمن السيبراني تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في المنشأة، وفقا لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية، وضمان العمل على تطبيقها ومراجعتها وتحديثها على فترات زمنية مخطط لها، على أن يتم تنفيذ إجراءات تقييم مخاطر الأمن السيبرانى بحد أدنى في الحالات التالية: • في المراحل المبكرة من المشاريع التقنية. • قبل إجراء أي تغيير جوهري في البنية التقنية. • عند التخطيط للحصول على خدمات طرف خارجي. • عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

6	**الأمن السيبراني ضمن إدارة المشاريع التقنية والمعلوماتية**	- يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في المنشأة، لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني ومراجعتها دوريا، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية، بحد أدنى ما يلى: • تقييم الثغرات ومعالجتها. • إجراء مراجعة للإعدادات والتحصين قبل إطلاق وتدشين المشاريع . • استخدام معايير التطوير الآمن للتطبيقات. • استخدام مصادر مرخصة وموثوقة لتطوير التطبيقات. • إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية.
7	**الالتزام بتشريعات ومعايير الأمن السيبراني**	- يجب على المنشأة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني، وأي اتفاقيات أو إلتزامات دولية معتمدة محليا تتضمن متطلبات خاصة بالأمن السيبراني.
8	**المراجعة والتدقيق الدورى للأمن السيبراني**	- يجب على الإدارة المعنية بالأمن السيبراني في المنشأة مراجعة تطبيق ضوابط الأمن السيبراني دوريا، وأن تتم عملية المراجعة أيضا من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني بشكل مستقل يراعى فيه عدم تعارض المصالح، ووفقا للمعايير العامة المقبولة للمراجعة، مع توثيق نتائج عملية المراجعة والتي يجب أن تتضمن نطاق عملية المراجعة، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وأن يتم عرضها على اللجنة الإشرافية للأمن السيبراني ومجلس الإدارة.
9	**الأمن السيبراني المتعلق بالموارد البشرية**	- يجب تحديد وتوثيق وإعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند إنتهاء/إنهاء عملهم بالمنشأة وبحد أدنى ما يلى: • تضمين مسئوليات الأمن السيبراني في عقود العاملين بالجهة. • إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني. • تطبيق متطلبات الأمن السيبراني والإلتزام بها. • مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد إنتهاء/إنهاء خدمتهم.
10	**التدريب والتوعية بالأمن السيبراني**	- يجب تطوير واعتماد برنامج دورى للتوعية بالأمن السيبراني في المنشأة، والتأكد من تزويد العاملين بالمنظمة بالمهارات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لتعزيز الوعي بالأمن السيبراني وتحدياته وبناء ثقافة إيجابية للأمن السيبراني، ويجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر السيبرانية وما يستجد منها، بما في ذلك: • التعامل الآمن مع خدمات البريد الإلكتروني وبصفة خاصة رسائل التصيد الإلكتروني. • التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. • التعامل الآمن مع خدمات تصفح الإنترنت ووسائل التواصل الإجتماعى.

المصدر: (إعداد الباحثة استنادا إلى الضوابط الأساسية الصادرة عن الهيئة الوطنية للأمن السيبراني– المملكة العربية السعودية، 2018)

ملحق 2: القواعد والعناصر الرئيسية للإفصاح عن إدارة مخاطر الأمن السيبراني

القاعدة	التفسير
1. الأهمية النسبية Materiality	- حيث يجب على منشآت الأعمال أن تأخذ في اعتبارها مدى أهمية حوادث الأمن السيبراني ومخاطرها بالنسبة للمستثمرين عند إعداد الإفصاحات المطلوبة وفي الوقت المناسب، وذلك بناءا على طبيعتها ومداها ونطاق الضرر المحتمل الذي قد يلحق بسمعة المنشأة، أو أدائها المالي، أو علاقاتها مع الأطراف المختلفة.
2. عوامل الخطر Risk Factors	- يجب على منشآت الأعمال الإفصاح عن المخاطر المرتبطة بالحوادث السيبرانية والتي تعد من عوامل الخطر المؤثرة على الاستثمارات المالية للمنشأة، على أن يتضمن ذلك ما يلي: • الحوادث السيبرانية السابقة وشدة وتكرار حدوثها. • احتمالية وقوع الحوادث السيبرانية والحجم الكمي والنوعي لها، بما في ذلك التكاليف المحتملة والعواقب الأخرى الناتجة عن اختلاس الأصول أو المعلومات أو تلف البيانات أو تعطل العمليات. • مدى كفاية الإجراءات المتخذة للحد من مخاطر الأمن السيبراني والتكاليف المرتبطة بها. • الدعاوى القضائية وتكاليف العلاج المرتبطة بحوادث الأمن السيبراني.
3. الموقف المالي ونتائج العمليات Financial Condition and Results of Operations	- يجب على منشآت الأعمال الإفصاح عن أية أحداث من المحتمل أن يكون لها تأثير جوهرى على نتائج العمليات أو موقفها المالي، بما في ذلك التكاليف المرتبطة بجهود الأمن السيبراني كالتكاليف المرتبطة بتنفيذ التدابير الوقائية، والتكاليف الأخرى المرتبطة بحوادث الأمن السيبراني وما يرتبط بها من مخاطر، مثل تكاليف معالجة الأضرار الناتجة عن الحوادث السيبرانية وتكاليف التقاضي وغيرها.
4. وصف طبيعة النشاط Description of Business	- يجب على منشآت الأعمال الإفصاح عن أية حوادث سيبرانية لها تأثير محتمل على منتجات المنشأة أو خدماتها أو علاقاتها مع العملاء والموردين، ومناقشة المخاطر المرتبطة بها بحسب طبيعة نشاط المنشأة.
5. الإجراءات القانونية Legal Proceedings	- يجب على منشآت الأعمال الإفصاح عن المعلومات المتعلقة بالإجراءات القانونية ذات الصلة بالدعاوى القضائية المرتبطة بحوادث الأمن السيبراني التي تتعرض لها.
6. الإفصاح في القوائم المالية Financial Statement Disclosures	- يجب على منشآت الأعمال أن تأخذ في اعتبارها عند إعداد القوائم المالية نطاق وحجم التأثيرات المالية لحوادث الأمن السيبراني، ودمجها في الوقت المناسب مع البيانات المالية المفصح عنها، إذ قد تؤثر حوادث الأمن السيبراني والمخاطر المرتبطة بها على القوائم المالية، كأن تؤدى إلى زيادة المصروفات المتعلقة بالتحقيق والإخطار بالانتهاك والتقاضي، أو إنخفاض الإيرادات، أو زيادة المطالبات المتعلقة بالضمانات وعدم الوفاء بالعقود وغيرها من التأثيرات المالية المحتملة.
7. رؤية مجلس الإدارة Board Risk Oversight	- يجب على منشآت الأعمال تقديم توصيف لدور أعضاء مجلس الإدارة، وذلك فيما يتعلق بصياغة إستراتيجية الأمن السيبراني وتقييم وإدارة مخاطر الأمن السيبراني.

المصدر:(إعداد الباحثة إستنادا إلى SEC 2011, 2018)

ملحق (3)

الدراسة التجريبية

قسم المحاسبة

كلية التجارة– جامعة القاهرة

السيد الأستاذ ألفاضل/.....

تحية طيبة وبعد،،،

أتشرف بإحاطتكم علما بأنني بصدد القيام بدراسة عنوانها " **دور حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني وأثره على تحسين الأداء المالي: دراسة تجريبية على البنوك المقيدة بالبورصة المصرية** ".

وحتى تكتمل الدراسة بشقيها النظرى والتطبيقى, فإن الأمر يستلزم استطلاع آراء سيادتكم حول موضوع الدراسة.

لذا أرجو من سيادتكم التكرم بقراءة بعض المفاهيم الأساسية والحالات الإفتراضية المرفقة قبل البدء في الرد على الأسئلة المرفقة، وتؤكد الباحثة لسيادتكم حرصها الشديد على أن تعامل جميع الإجابات بمنتهى السرية، وأن يقتصر استخدامها على أغراض البحث العملي فقط. وسوف تقوم الباحثة بعد الإنتهاء من تحليل بيانات قوائم الاستقصاء بإرسال النتائج التي تم التوصل إليها لسيادتكم في حالة رغبتكم في ذلك.

ولكم مقدماً جزيل الشكر على اهتمامكم وحسن تعاونكم...

الباحثة

د. ناريمان اسماعيل البردونى

المدرس بقسم المحاسبة

كلية التجارة – جامعة القاهرة

القسم الأول: بيانات شخصية

- الإسم (اختيارى):.....
- الوظيفة:.....
- عدد سنوات مزاولة المهنة:.....
- المؤهل العلمي:.....

القسم الثاني: تعريف بعض المصطلحات ذات الصلة بموضوع الدراسة

1. **الهجمات الإلكترونية:** عمليات تستهدف اختراق نظم المعلومات الرقمية الخاصة بالأفراد أو المؤسسات بهدف سرقتها أو التعديل عليها أو إتلافها لأغراض إجرامية مختلفة، وذلك بالاعتماد على البرامج والتقنيات الحديثة في مجال تكنولوجيا المعلومات.
2. **الأمن السيبراني:** عملية مستمرة لتأمين الأنظمة المتصلة بشبكة الإنترنت متضمنة الأجهزة والبرامج والبيانات من الهجمات الإلكترونية، والتعافي منها حال حدوثها، وذلك على نحو يضمن الحفاظ على سرية البيانات وسلامتها وتوافرها.
3. **مخاطر الأمن السيبراني:** الخسائر المحتمل حدوثها بسبب الهجمات الإلكترونية وما تحدثه من أضرار تتعلق بسرية ونزاهة وتوافر المعلومات، والتي تكبد منشآت الأعمال خسائر مالية كبيرة.
4. **حوكمة الأمن السيبراني:** مجموعة من الممارسات المناسبة لضبط وتوجيه أعمال المنشأة لتعزيز الأمن السيبراني والمرونة في مواجهة الهجمات الإلكترونية، بما يضمن منع أو التقليل من حدوثها، مع القدرة على اكتشافها والتعامل معها وسرعة التعافي من آثارها وتجنب تكرار حدوثها.

القسم الثالث: بيانات الدراسة التجريبية

الحالة الأولى

- يعتبر البنك (س) من أكبر بنوك القطاع الخاص المدرجة ببورصة تداول الأوراق المالية المصرية، حيث يقوم بتقديم مجموعة كبيرة ومتميزة من المنتجات والخدمات البنكية لعملائه، ويتضمن ذلك أكثر من 500 شركة من كبرى المؤسسات والشركات التي تعمل في مِصر بمختلف أنواعها. وبفضل علامته التِجارية الرائدة، نجح البنك (س) في تقديم أفضل الحلول المالية لعملائه من الأفراد والشركات الصغيرة

والمُتوسطة، وهو ما مكنه من جذب المزيد من العملاء الجُدد، ليحافظ بذلك على مركزه كأكثر البنوك التجارية تحقيقًا للأرباح في مصر، وفيما يلى القوائم المالية المختصرة للبنك (س) عن السنة المالية المنتهية في 2023/12/31.

قائمة المركز المالي المختصرة في 2023/12/31

بيان	2023/12/31	2022/12/31
إجمالى الأصول	834,866,099	635,831,917
إجمالى الإلتزامات	744,244,633	567,493,749
إجمالى حقوق الملكية	90,641,466	68,338,168
إجمالى الإلتزامات وحقوق الملكية	834,866,099	635,831,917

قائمة الدخل المختصرة عن السنة المالية المنتهية في 2023/12/31

بيان	2023/12/31	2022/12/31
صافي الدخل من العائد	52,929,662	31,004,898
صافي الدخل من الأتعاب والعمولات	5,438,225	3,078,137
الربح قبل ضرائب الدخل	41,653,373	23,941,286
صافي أرباح العام	29,668,865	16,172,150
ربحية السهم (جنيه/سهم)	8,59	4,80

قائمة التدفقات النقدية المختصرة عن السنة المالية المنتهية في 2023/12/31

بيان	2023/12/31	2022/12/31
صافي التدفقات النقدية من أنشطة التشغيل	174,305,009	64,902,547
صافي التدفقات النقدية من أنشطة الاستثمار	(34,692,176)	(32,438,527)
صافي التدفقات النقدية من أنشطة التمويل	(1,735,554)	(560,316)
النقدية وما في حكمها	234,317,913	92,969,526

قائمة التغيرات في حقوق الملكية المختصرة عن السنة المالية المنتهية في 2023/12/31

بيان	2023/12/31	2022/12/31
راس المال المصدر والمدفوع	30,355,083	30,355,083
احتياطيات	30,144,699	21,407,920
ارباح (خسائر) محتجزة	29,993,331	16,393,841
فروق ترجمة عملات اجنبية	148,353	181,324
اجمالى حقوق الملكية	90,641,466	68,338,168

ونظرا لاهتمام الساحة الاقتصادية العالمية بموضوع الأمن السيبراني، وذلك لارتفاع حدة الهجمات الإلكترونية على مختلف قطاعات الأعمال وبصفة خاصة القطاع المصرفي في مختلف أنحاء العالم، حيث أصبحت الهجمات الإلكترونية تشكل خامس أكبر التهديدات للاقتصاد العالمي، والتي من المرجح أن تصل تكلفتها إلى نحو 10 تريليون دولار بحلول عام 2025. فقد قرر البنك (س) العمل على تعزيز ثقافة الأمن السيبراني ورفع الوعى بمخاطر الهجمات الإلكترونية، وذلك من خلال اتخاذ العديد من التدابير والإجراءات لتفعيل حوكمة الأمن السيبراني، وذلك لمواجهة الهجمات الإلكترونية، على نحو يضمن المنع أو التقليل من حدوثها إلى جانب سرعة التعافي من آثارها.

السؤال الأول: بصفتك محاسبا ماليا أو مراجعا داخليا بالبنك، وفي ضوء قراءة ما تقدم، في رأيك .. هل تسهم التدابير والإجراءات التي يخطط البنك (س) تنفيذها – والموضحة بالجدول التالي – بشكل إيجابي في الحد من مخاطر الهجمات الإلكترونية؟

م	ضوابط حوكمة الأمن السيبراني	اوافق تماما	اوافق	محايد	غير موافق	غير موافق تماما
1	قيام مجلس إدارة البنك بتحديد وتوثيق واعتماد إستراتيجية للأمن السيبراني، وتنفيذ برنامج عمل لتطبيقها، ومراجعتها على فترات زمنية مخطط لها.					
2	إنشاء إدارة معنية بالأمن السيبراني في البنك وأن تكون مستقلة عن إدارة تكنولوجيا المعلومات والاتصالات، مع تشكيل لجنة إشرافية للأمن السيبراني بتوجيه من مجلس الإدارة على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها.					
3	قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات، وتوثيقها واعتمادها من مجلس الإدارة، ونشرها إلى ذوي العلاقة من العاملين في البنك والأطراف المعنية بها والعمل على ضمان تطبيقها، ومراجعتها على فترات زمنية مخطط لها.					
4	قيام مجلس إدارة البنك بتحديد وتوثيق واعتماد الهيكل التنظيمى للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للبنك وتقديم الدعم اللازم لإنفاذ ذلك، مع مراجعة هذه الأدوار والمسئوليات وتحديثها على فترات زمنية مخطط لها.					
5	قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني بالبنك وفقا لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية، وضمان العمل على تطبيقها ومراجعتها وتحديثها على فترات زمنية مخطط لها.					
6	تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في البنك لضمان تحديد مخاطر الأمن السيبراني					

	ومعالجتها كجزء من دورة حياة المشروع التقني ومراجعتها دوريا.					
7	إلتزام البنك بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني، وأي اتفاقيات أو التزامات دولية معتمدة محليا تتضمن متطلبات خاصة بالأمن السيبراني.					
8	مراجعة تطبيق ضوابط الأمن السيبراني بالبنك دوريا، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني بشكل مستقل يراعى فيه عدم تعارض المصالح ووفقا للمعايير العامة المقبولة للمراجعة والتدقيق، مع توثيق نتائج عملية المراجعة.					
9	تحديد وتوثيق وإعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند إنتهاء/إنهاء عملهم بالبنك.					
10	تطوير واعتماد برنامج دورى للتوعية بالأمن السيبراني في البنك، والتأكد من تزويد العاملين بالبنك بالمهارات والدورات التدريبية المطلوبة في مجال الأمن السيبراني.					

الحالة الثانية

نظرا لشكاوى المستثمرين وغيرهم من أصحاب المصالح من عدم وجود معلومات كافية وفي الوقت المناسب عن مخاطر الأمن السيبراني التي يتعرض لها البنك، وجهوده في إدارة تلك المخاطر، وبالتالي عدم قدرتهم على تقييم موقف الأمن السيبراني لديه ومعرفة مدى فعالية برامجه في إدارة تلك المخاطر، خاصة وقد اهتم عدد من المنظمات والهيئات المهنية الدولية بإصدار الإرشادات والأطر لدعم إفصاح منشآت الأعمال عن مخاطر الأمن السيبراني وبرنامج إدارتها، فإن البنك (س) يخطط للإفصاح عن إدارة مخاطر الأمن السيبراني.

السؤال الثاني: في ضوء قراءة ما تقدم، وبافتراض قيام البنك بتطبيق ضوابط حوكمة الأمن السيبراني ، في رأيك .. هل يسهم تطبيق ضوابط حوكمة الأمن السيبراني بشكل إيجابي في تشجيع البنك على الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني، باعتبار أن هذا التطبيق في حد ذاته، يمثل ذلك الجزء من الإفصاح الذي يعمل على بث إشارات إيجابية بشأن الجهود المبذولة من قبل المنشأة لتقليل مخاطر الأمن السيبراني أو الحد منها ومنعها؟ برجاء حدد ما يلى:

أوافق تماما	أوافق	محايد	غير موافق	غير موافق تماما

الحالة الثالثة

بافتراض أن البنك (س) قام بالإفصاح عن تقرير إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن السيبراني، وذلك على النحو التالي:

تقرير إدارة مخاطر الأمن السيبراني للبنك (س) لعام 2023

إلى السادة/ مساهمي البنك (س)

يحتل البنك (س) مكانة متقدمة في القطاع المالي عبر مجموعة من المؤشرات الهامة، ليؤكد مجدداً على موقعه الراسخ كقوة مالية ومؤسسة مصرفية وطنية رائدة، وقد سجل البنك (س) عاماً استثنائياً تميز بأداء مالى قياسي على صعيد الدخل والمركز المالي، وحقق تقدماً ملحوظاً نحو إنجاز أهدافه الاستراتيجية، وذلك من خلال حزمة من الإنجازات المالية الرئيسية التي تعكس متانة أدائه وكفاءة استراتيجيته.

وإيمانا من البنك بأهمية وضمان حماية أصوله المعلوماتية من الدخول غير المصرح به، أو التعديل، أو الفقدان، أو السرقة أو إساءة الاستخدام، سواء كان ذلك بصورة متعمدة تخريبية أو عرضية غير مقصودة. فقد قام البنك باعتماد إطار عمل لإدارة مخاطر الأمن السيبراني قائما على تطبيق ضوابط حوكمة الأمن السيبراني؛ وهى مجموعة من الممارسات المناسبة لضبط وتوجيه أعمال المنشأة لتعزيز الأمن السيبراني والمرونة في مواجهة الهجمات الإلكترونية، بما يضمن منع أو التقليل من حدوثها، مع القدرة على اكتشافها والتعامل معها وسرعة التعافي من آثارها وتجنب تكرار حدوثها، والتي تتضمن:

- قيام مجلس إدارة البنك بتحديد وتوثيق واعتماد إستراتيجية للأمن السيبراني، وتنفيذ برنامج عمل لتطبيقها، ومراجعتها على فترات زمنية مخطط لها.
- إنشاء إدارة معنية بالأمن السيبراني في البنك وأن تكون مستقلة عن إدارة تكنولوجيا المعلومات والاتصالات، مع تشكيل لجنة إشرافية للأمن السيبراني بتوجيه من مجلس الإدارة على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها.
- قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات، وتوثيقها واعتمادها من مجلس الإدارة، ونشرها إلى ذوي العلاقة من العاملين في البنك والأطراف المعنية بها والعمل على ضمان تطبيقها، ومراجعتها على فترات زمنية مخطط لها.
- قيام مجلس إدارة البنك بتحديد وتوثيق وإعتماد الهيكل التنظيمى للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للبنك وتقديم الدعم اللازم لإنفاذ ذلك، مع مراجعة هذه الأدوار والمسئوليات وتحديثها على فترات زمنية مخطط لها.
- قيام الإدارة المعنية بالأمن السيبراني في البنك بتحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني بالبنك وفقا لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية، وضمان العمل على تطبيقها

ومراجعتها وتحديثها على فترات زمنية مخطط لها.

- تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في البنك لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني ومراجعتها دوريا.
- إلتزام البنك بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني، وأي اتفاقيات أو التزامات دولية معتمدة محليا تتضمن متطلبات خاصة بالأمن السيبراني.
- مراجعة تطبيق ضوابط الأمن السيبراني بالبنك دوريا، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني بشكل مستقل يراعى فيه عدم تعارض المصالح ووفقا للمعايير العامة المقبولة للمراجعة والتدقيق، مع توثيق نتائج عملية المراجعة.
- تحديد وتوثيق وإعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند إنتهاء/إنهاء عملهم بالبنك.
- تطوير واعتماد برنامج دورى للتوعية بالأمن السيبراني في البنك، والتأكد من تزويد العاملين بالبنك بالمهارات والدورات التدريبية المطلوبة في مجال الأمن السيبراني.

هذا، وبفضل فعالية تلك الضوابط في تعزيز الأمن السيبراني للبنك وحماية أصوله المعلوماتية، فقد تمكن البنك من التصدي لإحدى هجمات حجب الخدمة (Attacks DDos)، التي كان قد تعرض لها خلال العام المالي المنتهي في 2023/12/31، حيث إستطاع البنك تدارك الأمر سريعا والسيطرة على الوضع، مع الحفاظ على سلامة كافة المعطيات الخاصة بالنظام المعلوماتي الخاص به.

وتؤكد إدارة الأمن السيبراني بالبنك على فعالية برنامج إدارة مخاطر الأمن السيبراني في تحقيق الأهداف السيبرانية التي يسعى إلى تحقيقها، وأنه قد تم إعداد هذا التقرير وفق متطلبات إطار الإفصاح عن إدارة مخاطر الأمن السيبراني الصادرة عن المعهد الأمريكي للمحاسبين القانونيين (AICPA) في عام 2017، وأنه قد تم مراجعة تطبيق ضوابط الأمن السيبراني بالبنك دوريا، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني بشكل مستقل يراعى فيه عدم تعارض المصالح ووفقا للمعايير العامة المقبولة للمراجعة والتدقيق، وقد أبدى مراقب الحسابات رأيا نظيفا في تقرير إدارة مخاطر الأمن السيبراني وفعالية تطبيق ضوابط الأمن السيبراني بالبنك.

التوقيع

رئيس مجلس الإدارة

والعضو المنتدب

2023/21/ 31

السؤال الثالث: في ضوء الإطلاع على تقرير إدارة مخاطر الأمن السيبراني السابق، ، في رأيك .. هل يسهم الإفصاح عن إدارة مخاطر الأمن السيبراني في ظل تطبيق ضوابط حوكمة الأمن السيبراني بشكل إيجابي في تحقيق المنافع التالية:

م	المنافع	اوافق تماما	اوافق	محايد	غير موافق	غير موافق تماما
1	الحفاظ على سمعة البنك وزيادة ثقة المتعاملين معه مما يسهم في تحسين الأداء المالي للبنك.					
2	زيادة ملائمة وموثوقية المعلومات المالية، مما يؤدي إلى جذب مزيد من العملاء وتحقيق قدر أكبر من العوائد.					
3	زيادة رضاء العملاء الحاليين وجذب مزيد من العملاء المستقبليين					
4	الحد من الغش والتلاعب المالي الإلكتروني ، مما ينعكس بالإيجاب على كفاءة الأداء المالي للبنك					
5	رفع كفاءة نظم الرقابة والمراجعة الداخلية وتحسين قدرتها على متابعة وتقييم ضوابط الأمن السيبراني لحماية أمن المعلومات المالية، مما يسهم في تحسين الأداء المالي للبنك.					
6	تمكين العملاء وغيرهم من أصحاب المصالح من تقييم قدرة البنك على التصدي للتهديدات السيبرانية ومعالجتها، ومن ثم تعزيز الثقة في الخدمات المصرفية المقدمة، وهو ما يعمل بدوره على جذب مزيد من العملاء، ومن ثم زيادة المدخرات وإرتفاع نسب السيولة لدى البنك وبالتالي تحسين أدائه المالي.					

لقد خصص هذا القسم لإبداء أي ملاحظات أو مقترحات من قبل سيادتكم فما يتعلق بموضوع الدراسة.....

.....

.....

.....

.....

في حالة رغبة سيادتكم في الحصول على نسخة من نتائج هذا البحث فبرجاء التواصل عبر البريد الإلكتروني: Nariman_ismail@yahoo.com